COURS DE L'INSTITUT FOURIER

ARMAND BRUMER

IV- Points rationnels sur les courbes modulaires et leurs jacobiennes

Cours de l'institut Fourier, tome 10 (1975), p. 139-212

<http://www.numdam.org/item?id=CIF_1975__10__A5_0>

IV - points rationnels sur les courbes modulaires et leurs jacobiennes

Dans tout ce chapitre, N désigne un nombre premier impair, et n le nombre $\frac{N-1}{(N-1,12)}$. Nous notons : Y,X,J,W, pour : $Y_o(N)$, $X_o(N)$, $J_o(N)$, W_N . Nos principales références sont [22] et [21] .

1. *ETUDE DE* $J_+(\mathbb{Q})$.

1.1. LE $\mathbb{Z}$-RANG DE $J_+(\mathbb{Q})$.

1.1.1. Notons $J_+ = (1+W)J$, et X_+ la courbe algébrique X/W ; remarquons que J_+ est annulé par $W-1$. Nous vérifions en (1.1.2) que J_+ est "presque" la jacobienne de X_+ . Notons g le genre de X , et g_+ celui de X_+ .

THEOREME. Le $\mathbb{Z}$-rang de $J_+(\mathbb{Q})$ est strictement positif dès que g_+ est strictement positif.

Nous montrons en (1.1.4) une partie de ce théorème. Nous calculons g_+ en (1.2), et montrons que g_+ est nul si et seulement si $N \leq 71$ et $N \neq 37,43,61,67$. D'où le résultat :

THEOREME (bis). Si N est supérieur ou égal à 73, ou si $N = 37,43,53,61,67$, alors $J_+(\mathbb{Q})$ est infini.

En (1.3) nous étudions les courbes hyperelliptiques, et nous montrons que g_+ est nul si et seulement si $X_o(N)$ est de genre 0 , ou de genre 1 (courbe elliptique), ou une courbe hyperelliptique différente de $X_o(37)$.

1.1.2. Comparons $J_+ = (1+W)J$, et $J(X_+) = J(X/W)$.

LEMME . Il existe une isogénie de $J(X_+)$ sur J_+ , rationnelle sur $\mathbb{Q}$, dont le noyau est d'exposant 2 .

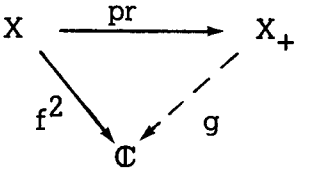
Rappelons qu'une isogénie entre deux variétés abéliennes de même dimension est un homomorphisme surjectif, c'est-à-dire un homomorphisme à noyau fini (cf.[43] , Appendix 10). Ici, nous ne savons pas que $J(X_+)$ et J_+ sont de même dimension ; nous allons donc construire un homomorphisme surjectif à noyau fini de $J(X_+)$ sur J_+ ; ce qui prouvera que $J(X_+)$ et J_+ ont même dimension et sont isogènes.

Rappelons des notations introduites au chapitre I : si Z désigne une courbe, on note $\mathcal{D}(Z)$ (resp. $\mathcal{D}_o(Z)$, $\mathcal{D}_\ell(Z)$), le groupe des diviseurs sur la courbe Z (resp. le sous-groupe des diviseurs de degré nul, des diviseurs de fonctions).

■ Considérons la projection (notée pr) de X sur $X_+ = X/W$, et notons et notons P_+ l'image d'un point P de X par cette projection ; l'image réciproque de P_+ est l'ensemble $\{P,WP\}$. Considérons l'homomorphisme de $\mathcal{D}(X_+)$ dans $\mathcal{D}(X)$ défini par : $(P_+) \longmapsto (P) + (WP) = (1+W).(P)$; c'est un homomorphisme, d'image $(1+W)\mathcal{D}(X)$. Sa restriction à $\mathcal{D}_o(X_+)$ est un homomorphisme de $\mathcal{D}_o(X_+)$ dans $\mathcal{D}_o(X)$, d'image $(1+W)\mathcal{D}_o(X)$. Sa restriction à $\mathcal{D}_\ell(X_+)$ est un homomorphisme de $\mathcal{D}_\ell(X_+)$ dans $\mathcal{D}_\ell(X)$. Nous obtenons ainsi un homomorphisme de $\mathcal{D}_o(X_+)/\mathcal{D}_\ell(X_+)$ dans $\mathcal{D}_o(X)/\mathcal{D}_\ell(X)$, dont l'image est égale à $(1+W).\mathcal{D}_o(X)/\mathcal{D}_\ell(X)$; autrement dit, nous obtenons un homomorphisme surjectif de $J(X_+)$ sur J_+ .

Etudions le noyau de cet homomorphisme ; il est formé des classes (modulo $\mathcal{D}_\ell(X_+)$) des diviseurs de degré nul sur X_+ dont l'image dans

$\mathcal{D}_0(X)$ est le diviseur d'une fonction sur X . Notons $\sum(P_+)$ un tel diviseur, $(1+W)\sum(P)$ son image dans $\mathcal{D}_0(X)$, et f une fonction sur X telle que $(f) = (1+W)\sum(P)$. Alors les fonctions f et $f\circ W$ ont même diviseur, donc il existe une constante C telle que $f = C.f\circ W$; et $f\circ W = C.f\circ W^2 = C.f$, donc $f = C^2 f$, d'où $C^2 = 1$. Ainsi, $f^2 = (f\circ W)^2 = f^2\circ W$, et il existe une fonction g sur X_+ telle que $g\circ pr = f^2$; comme $(f^2) = 2(1+W)\sum(P)$, le diviseur de g est égal à : $(g) = 2\sum(P_+)$, donc l'image de $2\sum(P_+)$ dans $J(X_+)$ est nulle. Ceci prouve que le noyau de l'homomorphisme de $J(X_+)$ sur J_+ est d'exposant 2 , donc qu'il est fini.



Enfin, on vérifie facilement que cette isogénie est définie sur $\mathbb{Q}$.∎

1.1.3. Admettons provisoirement le résultat suivant :

Les points rationnels du groupe de torsion de J sont contenus dans $J_- = (1-W)J$.

Ce résultat sera démontré (et précisé) en (3.2.4). Il implique le lemme suivant :

LEMME. Le groupe $2J(X_+)(\mathbb{Q})$ est sans torsion.

∎ Soit x un point rationnel de $J(X_+)$, tel que $2x$ soit un point de torsion ; nous voulons montrer que $2x$ est nul. Considérons l'isogénie transposée de l'isogénie construite en (1.1.2) : c'est un homomorphisme surjectif de J_+ sur $J(X_+)$, à noyau fini, défini sur $\mathbb{Q}$. Si y désigne un point de $J_+(\mathbb{Q})$ relevant x , alors un multiple de $2y$ est dans le noyau de l'isogénie ; comme ce noyau est fini, $2y$ est un point de torsion dans $2J_+(\mathbb{Q})$.

Donc il suffit de démontrer que $2J_+(\mathbb{Q})$ est sans torsion. Soit J^t le groupe de torsion de J ; nous avons admis que $J^t(\mathbb{Q})$ est inclus dans J_-.

Or J_- est annulé par $1+W$, et J_+ par $1-W$, donc $J_- \cap J_+$ est annulé par $(1+W) + (1-W) = 2$; ainsi, $2(J_+ \cap J^t)(\mathbb{Q}) = 0$. Or $2(J_+ \cap J^t) = 2J_+ \cap J^t$ (si $2x$ est de torsion, alors x est de torsion !) , et en résumé $(2J_+ \cap J^t)(\mathbb{Q}) = 0$, autrement dit : $2J_+(\mathbb{Q})$ est sans torsion. ∎

1.1.4. Nous montrons ci-dessous que le $\mathbb{Z}$-rang de $J_+(\mathbb{Q})$ est strictement positif dès que N est assez grand ($N \geq 12\,364$). Ainsi, nous démontrons une partie du théorème (1.1.1).

∎ Tout d'abord, d'après le lemme (1.1.2), il suffit de construire un point d'ordre infini de $J(X_+)(\mathbb{Q})$ lorsque N est grand. Et d'après le lemme (1.1.3), il suffit de construire un point x de $J(X_+)(\mathbb{Q})$ tel que $2x$ soit non nul.

La première partie de la démonstration est la construction de points de $J(X_+)(\mathbb{Q})$, appelés points de Heegner ; la deuxième partie consiste à montrer que ces points ne sont pas annulés par 2 , lorsque N est assez grand.

(i) Construction des points de Heegner. Ecrivons N sous la forme : $N = a^2 + db^2$, où a,b,d sont des entiers positifs, et où d est sans facteur carré. Soient $K = \mathbb{Q}(\sqrt{-d})$, et R un ordre de K contenant $\sqrt{-d}$; alors N se décompose dans R en : $N = \pi.\bar{\pi}$, où $\pi = a + \sqrt{-d}\,b$ et $\bar{\pi} = a - \sqrt{-d}\,b$. Notons H le groupe des classes de R-idéaux propres. On sait qu'alors il existe une extension galoisienne K_R de K , telle que H soit isomorphe au groupe de Galois de K_R sur K (cf. [18] , 8.1).

A chaque classe d'idéaux γ de H , on associe un élément de $X_o(N)(K_R)$ en considérant le couple $(E_\gamma, C_{\gamma\pi})$ défini ci-dessous : soit $\mathfrak{A}_\gamma$ un R-idéal propre représentant la classe γ ; c'est un réseau de $\mathbb{C}$; on pose alors $E_\gamma = \mathbb{C}/\mathfrak{A}_\gamma$ et $C_{\gamma,\pi} = \pi^{-1}\mathfrak{A}_\gamma/\mathfrak{A}_\gamma$. Notons $E_{\gamma,\pi}$ le couple $(E_\gamma, C_{\gamma,\pi})$.

On montre que l'extension $K_R/\mathbb{Q}$ est galoisienne, et que l'on a : $\sigma\gamma = \gamma^{-1}\sigma$ pour tout élément γ de $\mathrm{Gal}(K_R/\mathbb{Q})$, si σ désigne la conjugaison complexe (cf. [18] , 10.3). En identifiant H et $\mathrm{Gal}(K_R/K)$, on vérifie que, pour tous γ et γ' dans H , on a :

$\gamma'.\varepsilon_{\gamma,\pi} = \varepsilon_{\gamma'\gamma,\pi}$; $\sigma.\varepsilon_{\gamma,\pi} = \varepsilon_{\gamma^{-1},\bar{\pi}}$; $W.\varepsilon_{\gamma,\pi} = \varepsilon_{\gamma,\bar{\pi}}$. La dernière formule prouve que l'image de $\varepsilon_{\gamma,\pi}$ dans $X_+ = X/W$ est indépendante du choix de π ; notons $\varepsilon_{\gamma,+}$ cette image. Les deux premières formules prouvent que le diviseur $\sum_{\gamma\in H} (\varepsilon_{\gamma,+})$ est rationnel sur $\mathbb{Q}$.

Comme les deux pointes 0 et ∞ de X sont échangées par W , X_+ a une seule pointe (notée ∞) , qui est rationnelle sur $\mathbb{Q}$. Notons h_R le cardinal de H , c'est-à-dire le nombre de classes de R-idéaux propres ; le diviseur $\sum_{\gamma\in H} (\varepsilon_{\gamma,+}) - h_R(\infty)$ de X_+ est de degré nul, et rationnel sur $\mathbb{Q}$. Son image dans $J(X_+)(\mathbb{Q})$ est notée D_R et appelée le <u>point de Heegner</u> associé à l'ordre R .

(ii) Pour montrer que $2D_R$ est non nul, raisonnons par l'absurde. Supposons que $2D_R = 0$; alors, il existe une fonction f dans $\mathbb{Q}(X_+)$, de diviseur $(f) = 2\sum_{\gamma\in H} (\varepsilon_{\gamma,+}) - 2h_R(\infty)$. On peut montrer que f induit une fonction $\tilde{f}$ de $\mathbb{F}_2(\tilde{X}_+)$, de diviseur $(\tilde{f}) = (\tilde{f})$ (le tilde indique la réduction moculo 2) : disons seulement que l'existence de $\tilde{f}$ est une conséquence des propriétés des schémas de Néron, dont nous parlerons en (3.1). Notons g la fonction de $\mathbb{F}_2(\tilde{X})$ qui relève $\tilde{f}$: $\tilde{X} \xrightarrow[g]{} \tilde{X}_+ \xrightarrow{\tilde{f}} \mathbb{P}^1(\mathbb{F}_2)$. La fonction g a pour degré : $\deg(g) = 2\deg(\tilde{f}) \leq 4h_R$; et ses pôles sont les images de pointes (0 et ∞) de X . L'image par g de $\tilde{Y}(\mathbb{F}_4)$ est donc contenue dans l'espace affine $A^1(\mathbb{F}_4)$: ainsi, le nombre de points de $\tilde{Y}(\mathbb{F}_4)$ est au plus égal à : $\deg(g) . \#A^1(\mathbb{F}_4)$, c'est-à-dire : $\#\tilde{Y}(\mathbb{F}_4) \leq 16h_R$; or le lemme (1.1.5) prouvera que : $\#\tilde{Y}(\mathbb{F}_4) \geq \frac{N+1}{12}$, d'où : $N < 192\, h_R$.

Choisissons maintenant pour R l'ordre maximal du corps $K = \mathbb{Q}(\sqrt{-d})$; alors h_R est égal au nombre de classes h de K , et on peut le majorer par la formule : $h \leq \frac{|\delta|^{1/2}}{\pi} \mathrm{Log}.|\delta|$ (où $\pi = 3,14...!$) (cf.1.1.6). Or δ est égal à d ou à $4d$, ce qui donne : $h \leq \frac{2}{\pi} d^{1/2} \mathrm{Log}.4d$. Enfin, d est n'importe quel nombre positif sans facteur carré tel que N s'écrive : $N = a^2 + db^2$. Choisissons pour a la

partie entière de $\sqrt{N}$, et pour d la partie sans facteur carré de $N-a^2$; alors $a > \sqrt{N}-1$, d'où : $d \leq N-a^2 < 2\sqrt{N}$.

En résumé, si $2D_R$ est nul dans $J(X_+)(\mathbb{Q})$, alors on a : $N < \frac{192.2}{\pi} \cdot 2^{1/2} \cdot N^{1/4} \cdot \mathrm{Log}\ 8N^{1/2}$, c'est-à-dire : $N < 12364$. Ainsi, $J(X_+)(\mathbb{Q})$ contient un point d'ordre infini lorsque N est assez grand. ∎

1.1.5. Le lemme suivant nous a servi (en 1.1.4), et nous servira plus loin, à démontrer qu'une propriété de $X(\mathbb{Q})$ (ou de $J(\mathbb{Q}),\ldots$), est vérifiée "pour N assez grand". Il est dû à Ogg [32] .

LEMME. Soit $\tilde{Y}$ la réduction modulo 2 de Y . Le nombre de points de $\tilde{Y}$ rationnels sur $\mathbb{F}_4$ est supérieur ou égal à $\frac{N+1}{12}$.

∎ Considérons la courbe elliptique (notée E) définie sur $\mathbb{Q}$ par l'équation : $y^2 + y = x^3$; son discriminant est : $\Delta = -27$; son invariant : $j = 0$. Comme Δ est impair, la réduction de E modulo 2 (notée $\tilde{E}$) est une courbe elliptique ; son équation est encore : $y^2 + y - x^3$; comme le coefficient de xy est nul, $\tilde{E}$ est supersingulière (cf.III,1.3.3). Nous avons vu en (II,5.5.4) que, sur $\mathbb{F}_4$, le Frobenius π_4 de $\tilde{E}$ est égal à (-2) . Soit C un sous-groupe d'ordre N de E : comme π_4 est un entier premier à N , C est invariant par π_4 ; et comme π_4 engendre le groupe de Galois de $\overline{\mathbb{F}_4}$ sur $\mathbb{F}_4$, cela montre que C est rationnel sur $\mathbb{F}_4$.

Il reste à compter les sous-groupes C de E correspondant à des couples (E,C) qui ne deviennent pas isomorphes sur $\mathbb{F}_4$ après réduction. Or le nombre de sous-groupes d'ordre N de E est égal à N+1 (car $E_N \simeq (\mathbb{Z}/N\mathbb{Z})^2$) ; et le groupe $\mathrm{Aut}\ \tilde{E}$ est d'ordre 24 (en effet, $p = 2$ et $j = 0$; cf.I,1.2.3) ; mais le stabilisateur de C dans $\mathrm{Aut}\ \tilde{E}$ contient $\{\pm 1\}$, donc le nombre de couples (E,C') qui deviennent isomorphes à (E,C) sur $\mathbb{F}_4$ (après réduction modulo 2) est au plus égal à 12 . Ainsi, le nombre de points distincts obtenus sur $\tilde{Y}(\mathbb{F}_4)$ est au moins égal à $\frac{N+1}{12}$. ∎

1.1.6. Nous indiquons ici comment on peut démontrer la formule de majoration du nombre de classes en fonction du discriminant (formule utilisée en 1.1.4) (d'après J.R. JOLY, [16 b]).

LEMME. Soit K un corps quadratique imaginaire de nombre de classes h et de discriminant δ. On a alors : $h \leq \frac{|\delta|^{1/2}}{\pi} \log|\delta|$.

■ Notons χ le caractère associé au corps quadratique K (cf.[2a], 3.8.2) : c'est un caractère modulo $|\delta|$, qui prend les valeurs : $+1$, -1, ou 0. Notons $L(1,\chi) = \sum_{n=1}^{+\infty} \frac{\chi(n)}{n}$; alors h, $|\delta|$ et $L(1,\chi)$ sont liés par la formule : $h = \frac{|\delta|^{1/2}}{\pi} L(1,\chi)$ (cf.[2a],5.4.1).

Il reste donc à majorer $L(1,\chi)$ par $\mathrm{Log}|\delta|$. Posons $A(n) = \sum_{m=1}^{n} \chi(m)$; alors $L(1,\chi) = \sum_{n=1}^{+\infty} A(n)(\frac{1}{n} - \frac{1}{n+1})$ et l'on a, pour tout entier $n \geq 1$: $|A(n)| \leq \frac{|\delta|-1}{2}$ et $|A(n)| \leq n$. Notons M la partie entière de $\frac{|\delta|-1}{2}$; alors :

$$L(1,\chi) \leq \sum_{n=1}^{M-1} n(\frac{1}{n} - \frac{1}{n+1}) + M \sum_{n=M}^{+\infty} (\frac{1}{n} - \frac{1}{n+1})$$

$$= \left(\sum_{n=1}^{M-1} \frac{1}{n+1}\right) + 1 = \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{M} + 1 \leq 1 + \mathrm{Log}.M .$$

Enfin, on a : $M \leq \frac{|\delta|-1}{2} < \frac{|\delta|}{2}$, donc $\mathrm{Log}\ M < \mathrm{Log}|\delta| - \mathrm{Log}\ 2$; comme $\mathrm{Log}\ 2 < 1$, cela donne: $L(1,\chi) < \mathrm{Log}|\delta|$. ■

1.2. CALCUL DE g_+.

1.2.1. Le revêtement $X \to X_+$ est de degré 2, de groupe de Galois $\langle W \rangle$. Les points de ramification sont les points fixes par W. Si ω est le nombre de ces points fixes, la formule de Riemann-Hurwitz donne :

LEMME. $g_+ = \frac{g+1}{2} - \frac{\omega}{4}$.

Rappelons que g a été déterminé en (I.4.2.3) : $g = [\frac{N+1}{12}]$ si $12 \nmid N-1$, et $g = \frac{N-1}{12} - 1$ si $12 \mid N-1$. Ainsi, par exemple

$g = 0$ si $N \leq 10$ ou $N = 13$;

$g = 1$ si $N = 11$, 17 , 19 ;

$g = 2$ si $N = 23$, 29 , 31 , 37 .

1.2.2. Rappelons un peu d'arithmétique [33] : soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique, avec d entier sans facteur carré. L'anneau des entiers de K est $\mathbb{Z} \oplus \mathbb{Z}\omega$, où $\omega = \sqrt{d}$ si $d \equiv 2$ ou $3 \pmod 4$ et $\omega = \frac{1+\sqrt{d}}{2}$ si $d \equiv 1 \pmod 4$. Le discriminant m de K est égal à $4d$ dans le premier cas, à d dans le second cas. Tout ordre R de K est de la forme $\mathbb{Z} \oplus f.\mathbb{Z}\omega$ pour un entier $f > 0$ appelé le conducteur de R ; le discriminant m' de R est égal à $f^2 m$.

Réciproquement, si R est un ordre dans un corps quadratique, de discriminant donné m' , on détermine d et f de la manière suivante : d est l'entier obtenu en divisant m' par ses facteurs carrés, et f est l'entier positif égal à $\sqrt{\frac{m'}{d}}$ si $d \equiv 1 \pmod 4$, à $\sqrt{\frac{m'}{4d}}$ si $d \equiv 2$ ou $3 \pmod 4$.

Cette remarque justifie la notation suivante : soit m le discriminant d'un ordre R d'un corps quadratique ; on note $h(m)$ le nombre de classes de R-idéaux propres.

1.2.3. Notons h le nombre de classes de $\mathbb{Q}(\sqrt{m})$.

PROPOSITION. Si $N \geq 5$, le nombre ω de points fixes de W est égal à :

$h(-4N) = h$ si $N \equiv 1 \pmod 4$;

$2h(-N) = 2h$ si $N \equiv 7 \pmod 8$;

$4h(-N) = 4h$ si $N \equiv 3 \pmod 8$.

■ Remarquons d'abord que W échange les pointes 0 et ∞ ; ainsi les points fixes de W sont dans $Y_o(N)$, et s'interprètent comme des classes de $\mathbb{Q}$-isomorphisme de couples (E,λ) , où λ est une isogénie de degré N définie sur E . Nous savons (cf.II.5.2.4) que $W((E,\lambda)) = (E',\lambda')$ si E' est l'image de E par λ , et λ' l'isogénie transposée de λ . Donc (E,λ) est fixe par W , si et seulement si (E,λ) et (E',λ') sont $\overline{\mathbb{Q}}$-isomorphes. Cela signifie que E est $\overline{\mathbb{Q}}$-isomorphe à E' , et qu'en identifiant E et E' par ce $\overline{\mathbb{Q}}$-isomorphisme, on peut considérer λ et λ' comme deux endomorphismes de E , liés par une relation de la forme $\lambda' = \epsilon\lambda$ pour un automorphisme ϵ de E .

Or nous savons que $\mathrm{Aut}\, E \simeq \mu_{2i}$ ($i = 1,2,$ou 3) (cf.I,1.2.2) ; ainsi, $\lambda = \pm\sqrt{\frac{N}{\epsilon}}$, avec $\epsilon \in \mu_{2i}$: cela montre que λ n'est pas entier rationnel. Mais alors, $\mathbb{Q}(\lambda)$ est quadratique imaginaire (cf.II,5.2.3), donc $\epsilon = -1$ et $\lambda = \pm\sqrt{-N}$. En résumé, les points fixes de W sont les classes de $\overline{\mathbb{Q}}$-isomorphisme de couples (E,λ) , où $\mathrm{End}\, E$ est un ordre de $\mathbb{Q}(\sqrt{-N})$ contenant $\sqrt{-N}$, et λ l'isogénie $(\pm\sqrt{-N})$. Comme (E,λ) et $(E,-\lambda)$ sont $\overline{\mathbb{Q}}$-isomorphes, le nombre ω de points fixes de W est égal au nombre de classes de $\overline{\mathbb{Q}}$-isomorphisme de courbes elliptiques E telles que $\mathrm{End}\, E$ soit un ordre R de $\mathbb{Q}(\sqrt{-N})$ contenant $\sqrt{-N}$. D'après les rappels faits en (1.2.2) , on doit avoir $R = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-N}$ si $N \equiv 1$ ou 2 (mod.4) , et $R = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-N}$ ou $\mathbb{Z} \oplus \mathbb{Z}\,\frac{1+\sqrt{-N}}{2}$ si $N \equiv 3$ (mod.4) . Et, d'après la théorie de la multiplication complexe (cf.II,5.3.3), le nombre de classes de $\overline{\mathbb{Q}}$-isomorphisme de courbes E telles que $\mathrm{End}\, E \simeq R$ est égal au nombre de classes de R-idéaux propres. Ainsi, $\omega = h(-4N)$ si $N \not\equiv 3$ (mod.4) et $\omega = h(-N) + h(-4N)$ si $N \equiv 3$ (mod.4) ; de plus, $h = h(-4N)$ si $N \equiv 3$ (mod.4) , et $h = h(-N)$ si $N \equiv 3$ (mod.4) . Lorsque $N \equiv 3$ (mod.4), on peut calculer $h(-4N)$ en fonction de $h(-N)$, grâce à la formule suivante (cf.[18] ,8.1, th.7)

$$h_c = h.f.\frac{1}{(R^* : R_f^*)} \prod_{p|f} \left[1 - \left(\frac{K}{p}\right)p^{-1}\right]$$

où K est un corps quadratique, R l'ordre maximal de K , c un entier strictement positif, R_f l'ordre de conducteur f , h (resp. h_f) le nombre

de classes d'idéaux de K (resp. de classes de R_f-idéaux propres), et où le symbole $(\frac{K}{p})$ vaut +1 (resp. -1 , resp. 0) lorsque le nombre premier p est décomposé (resp. inerte, resp. ramifié) dans K .

Nous appliquons cette formule à $K = \mathbb{Q}(\sqrt{-N})$, $N \equiv 3 \pmod 4$, $R = \mathbb{Z} \oplus \mathbb{Z}\,\frac{1+\sqrt{-N}}{2}$, $f = 2$, $R_2 = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-N}$, $h = h(-N)$, $h_2 = h(-4N)$; nous savons que $(\frac{K}{2})$ est égal à +1 si $N \equiv 7 \pmod 8$, et à -1 si $N \equiv 3 \pmod 8$ (cf.[33] , 5.4) ; nous savons aussi que $R^* = R_2^* = \{\pm 1\}$ dès que $N \geq 5$ (cf.[33] ,4.5). D'où $h(-4N) = h(-N)$ si $N \equiv 7 \pmod 8$, et $h(-4N) = 3h(-N)$ si $N \equiv 3 \pmod 8$. ∎

1.2.4. *PROPOSITION* . Les nombres N tels que g_+ soit nul sont les suivants :

$N = 2,3,5,7,13$ $(g = 0)$; $N = 11,17,19$ $(g = 1)$;
$N = 23,29,31$ $(g = 2)$; $N = 41$ $(g = 3)$;
$N = 47$ $(g = 4)$; $N = 59$ $(g = 5)$;
$N = 71$ $(g = 6)$.

∎ Montrons d'abord que N est "petit" si g_+ est nul : en effet, le revêtement canonique : $X \to X_+ = X/W$ est défini sur $\mathbb{Q}$ et de degré 2 . Lorsque X_+ est de genre nul, ce revêtement définit une fonction de $\mathbb{Q}(X)$ de degré 2 . On peut montrer, comme en (1.1.4), que cette fonction induit, lorsqu'on réduit modulo 2 , une fonction de $\mathbb{F}_2(\tilde{X})$ de degré 2. L'image de $\tilde{X}(\mathbb{F}_4)$ par cette fonction est contenue dans $\mathbb{P}^1(\mathbb{F}_4)$, d'où : $\#\tilde{X}(\mathbb{F}_4) \leq 2 \times \#\mathbb{P}^1(\mathbb{F}_4)$ c'est-à-dire : $\#\tilde{X}(\mathbb{F}_4) \leq 10$. Comme $\tilde{X}(\mathbb{F}_4)$ contient $\tilde{Y}(\mathbb{F}_4)$ et les 2 pointes, et comme : $\#\tilde{Y}(\mathbb{F}_4) \geq \frac{N+1}{12}$ (cf. 1.1.5), on obtient: $\frac{N+1}{12} + 2 \leq 10$, c'est-à-dire $N < 96$.

Maintenant, appliquons le lemme (1.2.1) : $g_+ = \frac{g+1}{2} - \frac{\omega}{4}$; si g vaut 0 ou 1 , cela prouve que g_+ est nul ; d'où la proposition pour $N < 23$. Enfin, lorsque $23 \leq N < 96$, on utilise le calcul de ω en fonction de h (cf.1.2.3). ∎

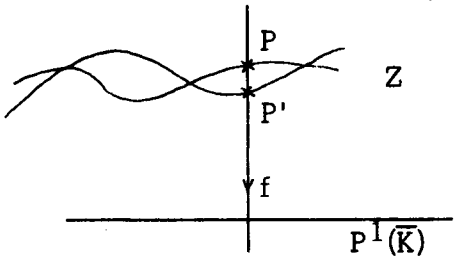
Remarque : en fait, pour montrer que $N < 96$, on utilise le fait que X est hyperelliptique lorsque $g_+ = 0$ (cf. 1.3.2 et 1.3.4).

1.3. COURBES HYPERELLIPTIQUES.

1.3.1. Une courbe algébrique Z , définie sur un corps K , de genre ≥ 2, est dite hyperelliptique s'il existe une fonction f de $\overline{K}(Z)$ de degré 2 , c'est-à-dire de diviseur $(f) = (P_1) + (P_2) - (Q_1) - (Q_2)$, avec $\{P_1,P_2\} \cap \{Q_1,Q_2\} = \phi$.

PROPOSITION. Une courbe Z de genre ≥ 2 est hyperelliptique si et seulement s'il existe une involution v de Z telle que Z/v soit de genre nul ; et alors v est l'unique involution de Z ayant cette propriété.

■ Soit f une fonction de $\overline{K}(Z)$ de degré 2 . Alors f définit un revêtement : $Z \to \mathbb{P}^1(\overline{K})$ de degré 2 .



Notons v le générateur du groupe de Galois de ce revêtement : ainsi, v est l'involution de Z qui fait correspondre à tout point P de Z , non ramifié dans $Z \to \mathbb{P}^1(\overline{K})$, l'unique point P' différent de P tel que $f(P) = f(P')$; et bien sûr $v(P) = P$ si le revêtement est ramifié en P . Alors Z/v est isomorphe à $\mathbb{P}^1(\overline{K})$, donc de genre nul.

Réciproquement, soit v une involution de Z telle que Z/v soit isomorphe à $\mathbb{P}^1(\overline{K})$. Comme le genre de Z est non nul, l'involution v est non triviale et définit un revêtement de degré 2 : $Z \to Z/v \simeq \mathbb{P}^1(\overline{K})$. Autrement dit, v définit une fonction f de $\overline{K}(Z)$ de degré 2 ; donc Z est hyperelliptique.

Soit maintenant w une autre involution de Z telle que Z/w soit de genre nul.

Soient P'_1 un point de Z non ramifié dans $Z \to Z/w$, et

$P'_2 = w(P'_1)$. La fonction $f' = \frac{1}{f-f(P'_1)}$ a pour diviseur

$$(f') = -(P'_1)-(P'_2) + (Q_1) + (Q_2) \ ;$$

elle est donc de degré 2 comme f . D'autre part, montrons qu'il existe une forme différentielle holomorphe ω sur Z de diviseur

$$(\omega) = (g-1)((P'_1)+(P'_2)) \ .$$

Considérons les diviseurs suivants : $D_1 = (g-1)((P'_1)+(P'_2))$, D_2 le diviseur d'une forme différentielle holomorphe sur Z , $D_3 = D_2-D_1$; alors $\deg(D_1) = \deg(D_2) = 2(g-1)$, $\deg(D_3) = 0$, et le théorème de Riemann-Roch donne : $\ell(D_3) = \ell(D_1) - (g-1)$; or, pour tout entier $i \geq 0$, la fonction f'^i a pour diviseur $i\left((Q_1)+(Q_2)-(P'_1)-(P'_2)\right)$: donc f'^i est dans $L\left(i\left((P'_1)+(P'_2)\right)\right)$, mais pas dans $L\left((i-1)((P'_1)+(P'_2))\right)$; ainsi, les fonctions 1 , f' , f'^2 , ... , f'^{g-1} sont linéairement indépendantes dans $L(D_1)$, d'où : $\ell(D_1) \geq g$, et $\ell(D_3) \geq 1$. Il existe donc une fonction g de diviseur supérieur ou égal à D_3 ; en fait, l'inégalité stricte impliquerait $\deg(g) > \deg(D_3)$, ce qui est impossible (ces deux degrés sont nuls !) . Donc $(g) = D_3$, et le diviseur D_1 est le diviseur d'une forme différentielle holomorphe sur Z , notée ω .

Alors $\omega \circ v' + \omega$ est une forme différentielle holomorphe sur Z/w , qui est de genre nul : donc $\omega \circ w = -\omega$, et les diviseurs $(\omega \circ w)$ et (ω) sont égaux. Cela signifie que $(g-1)((P'_1)+(P'_2)) = (g-1)\left((w(P'_1))+w(P'_2))\right)$ i.e. (rappelons que $g \geq 2$) que $(P'_1) + (P'_2) = (w(P'_1)) + (w(P'_2))$. Comme $P'_1 \neq w(P'_1)$, nous obtenons : $P'_2 = w(P'_1)$, i.e. $v(P'_1) = w(P'_1)$. Ainsi, v et w coïncident en tout point de Z non ramifié dans $Z \to Z/w$, ce qui prouve que $v = w$. ■

1.3.2. *COROLLAIRE*. Les courbes modulaires X de genre $g \geq 2$ telles que $g_+ = 0$ sont hyperelliptiques.

■ Ce sont les courbes X telles que W soit l'involution hyperelliptique. ■

1.3.3. *PROPOSITION*. Toute courbe Z de genre 2 est hyperelliptique.

▪ D'après (II,4.1.5) l'espace des formes différentielles holomorphes sur Z est de dimension $g = 2$. Soit $\{\omega,\omega'\}$ une base de cet espace ; chaque forme différentielle holomorphe sur Z est de degré $2g - 2 = 2$, donc la fonction ω/ω' sur Z a pour diviseur

$$(\frac{\omega}{\omega'}) = (\omega) - (\omega') = ((P_1)+(P_2)) - ((P_1')+(P_2')) ,$$

où $\{P_1,P_2\} \cap \{P_1',P_2'\}$ est vide car $\{\omega,\omega'\}$ sont linéairement indépendantes. Ainsi, ω/ω' est une fonction de degré 2 sur Z. ▪

1.3.4. Supposons $N \geq 23$, c'est-à-dire $g \geq 2$.

PROPOSITION. La courbe modulaire X est hyperelliptique si et seulement si N est inférieur ou égal à 71, et différent de 43, 53, 61, 67.

▪ Vu la proposition (1.2.4), cela signifie que les seules courbes X hyperelliptiques sont celles qui vérifient $g_+ = 0$, et la courbe $X_0(37)$. Comme $X_0(37)$ est de genre 2, le corollaire (1.3.2) et la proposition (1.3.3) prouvent que ces courbes sont bien hyperelliptiques.

La réciproque se démontre en 2 parties : tout d'abord, on montre que N est borné, en utilisant le raisonnement fait en (1.2.4) : X est un revêtement de degré 2 d'une courbe de genre nul, donc il existe une fonction de degré 2 dans $\mathbb{F}_2(\widetilde{X})$, et l'on a : $\#\widetilde{X}(\mathbb{F}_4) \leq 2.\#\mathbb{P}^1(\mathbb{F}_4) = 10$. Par ailleurs (cf.1.1.5) on a :

$$\#\widetilde{X}(\mathbb{F}_4) = \#\widetilde{Y}(\mathbb{F}_4) + 2 \geq \frac{N+1}{12} + 2 .$$

D'où : $N < 96$, ou encore (puisque N est premier) : $N \leq 89$.

Ensuite, on étudie séparément chacune des valeurs de N comprises entre 23 et 89 (cf. Ogg [32]). ▪

1.3.5. Remarque : Ogg [32] a étudié par la méthode ci-dessus toutes les

courbes modulaires $X_0(N)$ hyperelliptiques, sans supposer N premier. Il obtient 19 valeurs de N, la plus grande étant 71. L'involution hyperelliptique est modulaire (c'est-à-dire provient d'un automorphisme de $\mathcal{H}$) pour $N \neq 37$, et c'est l'involution d'Atkin-Lehner pour $N \neq 37, 40, 48$.

2. *POINTS D'ORDRE FINI DE* J_-.

Nous supposons toujours, désormais, J non trivial, c'est-à-dire $g \geq 1$, ou encore :

$$\boxed{N \geq 11 \text{ et } N \neq 13} \quad .$$

Puisque nous venons de voir que $J_+(\mathbb{Q})$ est généralement infini, nous allons étudier $J_-(\mathbb{Q})$, où $J_- = (1-W)J$. Remarquons que $J_+ + J_- = J$, et que le groupe $J_+ \cap J_-$ est d'exposant 2 (car W est une involution).

2.0. Comparons les variétés abéliennes $J_- = (1-W)J$ et $J^- = J/J_+ = J/(1+W)J$:

LEMME. Il existe une isogénie de J_- sur J^-, dont le noyau est d'exposant 2.

■ En composant l'injection canonique de J_- dans J, et la projection canonique de J sur $J^- = J/J_+$, on obtient un homomorphisme surjectif (car $J_- + J_+ = J$), de noyau fini et annulé par 2 (car ce noyau est égal à $J_- \cap J_+$). ■

Nous allons montrer (en 2.1 et 2.2) que J contient 2 sous-groupes cycliques d'ordre $\frac{N-1}{(N-1,12)} = n$, rationnels sur $\mathbb{Q}$, le premier étant composé de points rationnels sur $\mathbb{Q}$, et le second se comportant

comme μ_n sous l'action de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Ensuite, nous étudions l'action des opérateurs de Hecke et de l'involution d'Atkin-Lehner sur ces sous-groupes qui sont en fait "presque" des sous-groupes de J_- (en 2.3). Enfin, en (2.4), nous étudions le sous-anneau de End J engendré par les opérateurs de Hecke et d'Atkin-Lehner.

2.1. LE GROUPE "PARABOLIQUE" C .

2.1.1. *LEMME*. Il existe une forme modulaire (notée F) de poids (N-1) pour $\Gamma_0(N)$, et une forme modulaire (notée G) de type $(\frac{3}{2}(N-1), N, (\frac{\cdot}{N}))$, telles que F et G ne s'annulent qu'à la pointe 0 de X .

(voir en (II,1.1.1) la définition des formes modulaires de type (k,N,ϵ)) .

▪ Suivant Hecke et Fricke (cf.[14] , [9]), nous allons construire F et G à partir des fonctions de Weierstrass $\wp$ et $\wp'$.

(i) Pour tout couple d'entiers (r,s) dans $\mathbb{Z}^2 \setminus (N\mathbb{Z})^2$ (ici le signe \ désigne la différence ensembliste), définissons sur $\mathfrak{H}$ une fonction notée $h_{r,s}$ par : $$h_{r,s}(\tau) = \wp(\frac{r\tau+s}{N} ; \tau) = \wp(\frac{(r\ s)\binom{\tau}{1}}{N} ; \tau) .$$

Si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, alors

$$h_{r,s}(\gamma\tau) = \wp(\frac{(r\ s)\binom{\gamma\tau}{1}}{N} ; \gamma\tau) = (c\tau+d)^2 \wp(\frac{(r\ s)\gamma\binom{\tau}{1}}{N} ; \tau)$$

car $\{a\tau+b, c\tau+d\}$ et $\{\tau,1\}$ forment deux bases du même réseau de $\mathbb{C}$ (cf.I,2.1.8). Ainsi, si (r',s') est défini par : $(r'\ s') = (r\ s)\gamma$, on a : $h_{r,s} \mid_2 \gamma = h_{r',s'}$.

D'autre part, comme $\wp$ est $(\mathbb{Z}\tau \oplus \mathbb{Z})$-elliptique, la fonction $h_{r,s}$ ne dépend que des classes de r et s dans $(\mathbb{Z}/N\mathbb{Z})$. En particulier, si $r = 0$ et $\gamma \in \Gamma_0(N)$ (i.e. $c \equiv 0 \pmod N$) , nous obtenons : $(r',s') = (cs,ds)$,

et $h_{o,s}|_2\gamma = h_{o,ds}$, pour tout $s \in \mathbb{Z}\backslash N\mathbb{Z}$. De plus, la parité de $\wp(u;\tau)$ par rapport à u se traduit par : $h_{o,-s} = h_{o,s}$. Tout ceci nous amène à poser $h_s = h_{o,s}$, et à définir sur $\mathcal{H}$ la fonction :

$$F = \prod_{s=1}^{\frac{N-1}{2}} (h_s - h_{2s}) ,$$

lorsque N est au moins égal à 5 (nous verrons plus bas le cas $N = 3$). La fonction F est holomorphe sur $\mathcal{H}$; si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_o(N)$, alors

$$F|_{N-1}\gamma = \prod_{s=1}^{\frac{N-1}{2}} (h_s|_2\gamma - h_{2s}|_2\gamma) = \prod_{s=1}^{\frac{N-1}{2}} (h_{ds} - h_{2ds}) .$$

L'ensemble $\{1,2,\ldots,\frac{N-1}{2}\}$ forme un système de représentants de $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$; l'application de $\{1,2,\ldots,\frac{N-1}{2}\}$ dans lui-même qui associe à s le représentant de la classe de ds est une bijection, car d est premier à N . Ainsi, $F|_{N-1}\gamma = F$. Le développement de $\wp$ à l'infini, donné en (I,2.5.1), permet de calculer le développement de F aux deux pointes ∞ et 0 , et de vérifier que F y est holomorphe, s'annule en 0 , et ne s'annule pas à l'infini.

Si F s'annule en un point τ de $\mathcal{H}$, il existe un entier s tel que $\wp(\frac{s}{N};\tau) = \wp(\frac{2s}{N};\tau)$, c'est-à-dire tel que $s \equiv \pm 2s \pmod N$; comme $s \not\equiv 0 \pmod N$, et comme nous avons supposé $N \geq 5$, c'est impossible.

Enfin, lorsque $N = 3$, on pose $F = h_1$; c'est une forme modulaire de poids 2 pour $\Gamma_o(3)$, qui ne s'annule qu'en 0 .

(ii) De manière analogue et par abus de langage, posons $h'_{r,s}(\tau) = \wp'(\frac{r\tau+s}{N};\tau)$ pour tout couple $(r,s) \in \mathbb{Z}^2\backslash(N\mathbb{Z})^2$; si $\gamma \in \Gamma$ et si (r',s') est défini par $(r'\ s') = (r\ s)\gamma$, alors $h'_{r,s}|_3\gamma = h'_{r',s'}$; si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_o(N)$, alors $h'_{o,s}|_3\gamma = h'_{o,ds}$. Posons $h'_s = h'_{o,s}$, et $G = \prod_{s=1}^{\frac{N-1}{2}} h'_s$; alors $G|_{\frac{3}{2}(N-1)}\gamma = \varepsilon(d)G$, où $\varepsilon(d) = \pm 1$, car h' est

une fonction impaire (comme $\wp'$) . Calculons $\varepsilon(d)$: notons s' l'image de s dans la bijection de $\{1,2,\ldots,\frac{N-1}{2}\}$ sur lui-même induite par la multiplication par d dans $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$; pour chaque valeur de s , ou bien $s' \equiv ds \pmod N$ et $h_{s'} = h_{ds}$, ou bien $s' \equiv -ds \pmod N$ et $h_{s'} = -h_{ds}$. En résumé,

$$G|_{\frac{3}{2}(N-1)}\gamma = (-1)^r \prod_{s'=1}^{\frac{N-1}{2}} h_{s'} = (-1)^r G ,$$

où r est le nombre des s tels que $s' \equiv -ds \pmod N$: ainsi, $(-1)^r$ est congru (mod N) à $\prod_{s=1}^{\frac{N-1}{2}} \frac{ds}{s}$, c'est-à-dire à $d^{\frac{N-1}{2}}$; d'où $(-1)^r = (\frac{d}{N})$.

Enfin, le développement de $\wp'$ à l'infini donne celui de G en 0 et ∞ , et permet de voir que G est holomorphe au pointes, s'annule an 0 , et ne s'annule pas à l'infini. ∎

2.1.2. Par ailleurs, nous avons défini en (I,2.4.3) la fonction η de Dedekind, et montré que $\eta^{24} = \Delta$ est un générateur de l'espace des formes paraboliques de poids 12 pour Γ . Notons η_N la fonction définie sur $\mathcal{H}$ par : $\eta_N(\tau) = \eta(N\tau)$.

PROPOSITION. <u>La fonction</u> η^N/η_N <u>est une forme modulaire de type</u> $(\frac{N-1}{2}, N, (\frac{\cdot}{N}))$.

∎ (i) La fonction $(\eta^N/\eta_N)^{24}(\tau) = \frac{\Delta^N(\tau)}{\Delta(N\tau)}$ est holomorphe sur $\mathcal{H}$; son développement à l'infini est donné par :

$$\frac{q^N \prod_{n\geq 1}(1-q^n)^{24N}}{q^N \prod_{n\geq 1}(1-q^{Nn})^{24}} = 1 + \ldots ,$$

elle est donc holomorphe sur $\hat{\mathcal{H}}$ et non nulle à l'infini. Nous allons montrer que la fonction Δ_N (définie par $\Delta_N(\tau) = \Delta(N\tau)$) est une forme modulaire de poids 12 pour $\Gamma_o(N)$; cela prouvera que $(\eta^N/\eta_N)^{24}$ est une forme modulaire de poids $12(N-1)$ pour $\Gamma_o(N)$. Or, si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_o(N)$;

alors l'élément $\gamma' = \begin{pmatrix} a & Nb \\ c/N & d \end{pmatrix}$ appartient à Γ , et $N.\gamma(\tau) = \gamma'(N\tau)$; d'où $\Delta_N|_{12}\,\gamma(\tau) = \frac{1}{(c\tau+d)^{12}}\,\Delta(\gamma'(N\tau)) = \Delta|_{12}\,\gamma'(N\tau) = \Delta_N(\tau)$. De plus, $(\eta^N/\eta_N)^{24}$ ne s'annule qu'à la pointe 0 de X .

(ii) Cette étude de $(\eta^N/\eta_N)^{24}$, jointe au lemme (2.1.1), nous donne 3 formes modulaires de poids $12(N-1)$ pour $\Gamma_o(N)$, à savoir : $(\eta^N/\eta_N)^{24}$, F^{12} , et G^8 ; et ces formes ne s'annulent qu'en 0 . Le quotient de deux d'entre elles est une fonction sur X , avec 0 comme seul pôle ou zéro éventuel (donc n'ayant pas de zéro, ou pas de pôle !) : une telle fonction est une constante non nulle, et les trois formes $(\eta^N/\eta_N)^{24}$, F^{12} , G^8 sont proportionnelles. Cela prouve que les fonctions sur $\mathcal{H}$ $(\eta^N/\eta_N)^2$ et F (resp. $(\eta^N/\eta_N)^3$ et G) sont proportionnelles, donc que η^N/η_N est proportionnelle à G/F , et ceci démontre la proposition. ∎

2.1.3. *COROLLAIRE* . <u>Si</u> $N \equiv 11 \pmod{12}$, <u>la fonction</u> $\eta^2\eta_N^2$ <u>est une forme parabolique de poids</u> 2 <u>pour</u> $\Gamma_o(N)$.

∎ En effet, $\eta^2\eta_N^2$ est holomorphe sur $\mathcal{H}$ et aux pointes ; par ailleurs

$$\eta^2\eta_N^2 = \left(\frac{\eta_N}{\eta^N}\right)^2 . \eta^{2(N+1)} \quad \text{et} \quad \eta^{2(N+1)} = \Delta^{\frac{N+1}{12}}$$

est une puissance (entière) de Δ lorsque $N \equiv 11 \pmod{12}$. Ainsi $\eta^{2(N+1)}$ est une forme parabolique de poids $N+1$ pour $\Gamma_o(N)$, alors que $(\frac{\eta^N}{\eta_N})^2$ est une forme modulaire de poids $N-1$ pour $\Gamma_o(N)$ d'après la proposition (2.1.2). ∎

<u>Remarque</u> : nous avons admis ce résultat dans l'étude de $X_o(11)$ (cf. II.8.1).

2.1.4. Rappelons que $n = \frac{N-1}{(N-1,12)}$ est le numérateur de la fraction réduite $\frac{N-1}{12}$. Ogg a démontré le résultat suivant (cf. [27]).

THEOREME. L'élément $(0) - (\infty)$ de J engendre un sous-groupe cyclique d'ordre n de $J(\mathbb{Q})$.

■ Considérons la fonction $f = \frac{\Delta}{\Delta_N}$. Nous savons que Δ est une forme parabolique de poids 12 pour Γ , dont le développement de Fourier est à coefficients dans $\mathbb{Q}$. Cela implique que Δ_N est une forme modulaire de poids 12 pour $\Gamma_o(N)$ (voir la démonstration de (2.1.2)), et que f est une fonction modulaire de poids nul pour $\Gamma_o(N)$, dont le développement de Fourier est à coefficients dans $\mathbb{Q}$, - i.e. $f \in \mathbb{Q}(X)$ -, et dont le diviseur est une combinaison linéaire de (0) et (∞) . Or, à l'infini, $f(\tau) = \frac{q + \dots}{q^N + \dots}$, d'où le diviseur $(f) = (N-1)((0)-(\infty))$. Ainsi, l'image $\underline{d}$ de $(0) - (\infty)$ dans J est d'ordre fini divisant $(N-1)$. Notons n' l'ordre de $\underline{d}$, et montrons que $n' = n$.

Soit $h' = \frac{N-1}{n'}$: autrement dit, h' est le plus grand entier tel que $cf^{1/h'} \in \mathbb{Q}(X)$ pour une certaine constante c et pour un certain choix de la racine h'-ème. Mais pour tout entier k , le développement de Fourier de $f^{1/k}$ est à coefficients dans $\mathbb{Q}$, donc h' est le plus grand entier tel que $f^{1/h'}$ soit une forme modulaire pour $\Gamma_o(N)$. Or

$$f \mid_o W_N(\tau) = \frac{\Delta(\frac{-1}{N\tau})}{\Delta(\frac{-1}{\tau})} = \frac{\tau^{12} N^{12} \Delta(N\tau)}{\tau^{12} \Delta(\tau)}$$

puisque $\Delta \mid_{12} \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)(\tau) = \tau^{-12}\Delta(\frac{-1}{\tau})$; et $f \mid_o W_N \in \mathbb{Q}(X)$ car l'opérateur W_N est rationnel sur $\mathbb{Q}$. Ainsi, $N^{12/h'} = f^{1/h'}(f \mid_o W_N)^{1/h'} \in \mathbb{Q}((q))$, ce qui implique que h' divise 12 , donc que h' divise $(N-1,12)$; notons $h = (N-1,12)$. D'autre part

$$f^{1/h} = \left(\frac{\Delta}{\Delta_N}\right)^{1/h} = \left(\frac{\eta}{\eta_N}\right)^{24/h} = \left(\frac{\eta}{\eta_N}\right)^{N\,24/h} . \eta^{-24.\frac{N-1}{h}} .$$

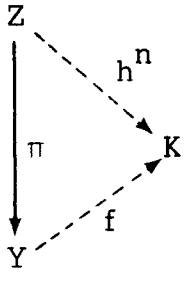
Comme h divise 12, la proposition (2.1.2) montre que $\left(\frac{\eta}{\eta_N}\right)^{N\,24/h}$ est une forme modulaire pour $\Gamma_o(N)$; et $\eta^{24\frac{N-1}{h}} = \Delta^{\frac{N-1}{h}}$ est aussi modulaire pour $\Gamma_o(N)$, car h divise $N-1$. En résumé, $h' = h$ et $n' = n$. ■

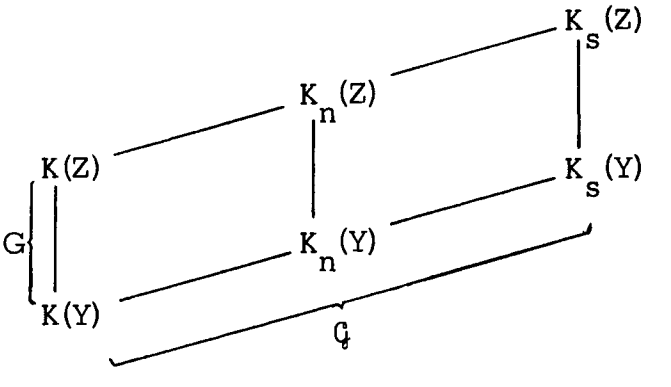
Ce sous-groupe $\langle (0)-(\infty) \rangle$ est noté C .

Nous montrerons en (3.2.4) que C est exactement le groupe de torsion de $J(\mathbb{Q})$.

2.2. LE GROUPE DE SHIMURA Σ . (cf.[27])

2.2.1. Soient K un corps et K_s une clôture séparable de K ; n un entier premier à la caractéristique de K ; Y et Z deux courbes non singulières, définies sur K , absolument irréductibles ; π un revêtement : $Z \to Y$, défini sur K . Notons μ_n le groupe des racines n-ème de l'unité dans K_s , et $K_n = K(\mu_n)$





PROPOSITION. Si le revêtement $Z \to Y$ est non ramifié , de degré n , galoisien, de groupe de Galois cyclique, alors il existe un sous-groupe de $J(Y)(K_n)$, isomorphe à μ_n en tant que $Gal(K_s/K)$-module.

■ L'extension $K_n(Z)/K_n(Y)$ est une extension de Kummer de degré n , donc il existe un élément h de $K_n(Z)$ tel que : $h^n = f \in K_n(Y)$, et $K_n(Z) = K_n(Y)(h)$ (cf [16,a] ,8.8). Montrons que le diviseur de f est de la forme $(f) = nD$: notons $(f) = \sum_{i=1}^{m} n_i P_i$, et $\pi^{-1} P_i = \sum_{j=1}^{n} Q_{i,j}$; le revêtement π étant non ramifié, tous les points $Q_{i,j}$ sont distincts ; la fonction $\pi^*(f) = f \circ \pi = h^n$ sur Z a pour diviseur :

$$(\pi^*(f)) = \sum_{i=1}^{m} \sum_{j=1}^{n} n_i Q_{ij} = n(h) \ ;$$

ainsi, n divise tous les n_i, et (f) est de la forme nD. De plus, n est le plus petit entier tel que nD soit le diviseur d'une fonction sur Y (sinon, le revêtement serait de degré $< n$).

Notons δ la classe de D dans $J(Y)(K_n)$, et Σ le sous-groupe de $J(Y)(K_n)$ engendré par δ ; nous venons de montrer que Σ est d'ordre n.

Etudions l'action de $\mathcal{G} = Gal(K_s/K)$ sur Σ. Notons G le groupe de Galois de $Z \to Y$, et définissons une application bilinéaire Φ de $\Sigma \times G$ dans μ_n par : $\Phi(\delta, \alpha) = \frac{\alpha(h)}{h}$ (en effet, $(\frac{\alpha(h)}{h})^n = \frac{\alpha(f)}{f} = 1$). Cette application Φ est non dégénérée et induit, pour tout générateur α de G, un isomorphisme de $\mathcal{G}$-modules, noté Φ_α, entre Σ et μ_n : l'action du groupe $\mathcal{G}$ sur h induit une action de $\mathcal{G}$ sur Σ définie par : si $\sigma \in \mathcal{G}$, alors δ^σ est la classe dans $J(Y)(K_n)$ du diviseur $D^\sigma = (h^\sigma)$. Vérifions que δ^σ est bien dans Σ : il est obtenu à partir de f^σ comme δ à partir de f ; or, d'après la théorie des extensions de Kummer, f^σ et f engendrent le même sous-groupe de $K_n(Y)^*$. Ainsi,

$$\Phi_\alpha(\delta^\sigma) = \frac{\alpha(h^\sigma)}{h^\sigma} ,$$

et même, puisque les éléments de G et $\mathcal{G}$ commutent,

$$\Phi_\alpha(\delta^\sigma) = (\frac{\alpha(h)}{h})^\sigma .$$

D'autre part, $\mathcal{G}$ agit sur μ_n de la manière suivante : pour tout σ dans $\mathcal{G}$, il existe un élément s de $(\mathbb{Z}/n\mathbb{Z})^*$ tel que l'on ait $\zeta^\sigma = \zeta^s$, quel que soit ζ dans μ_n. En particulier, on a $(\frac{\alpha(h)}{h})^\sigma = (\frac{\alpha(h)}{h})^s$, c'est-à-dire $\Phi_\alpha(\delta^\sigma) = \Phi_\alpha(s\delta)$, donc $\delta^\sigma = s\delta$.

En résumé, l'action de $\mathcal{G}$ sur Σ peut être décrite de la façon suivante : si $\sigma \in \mathcal{G}$, notons s l'élément de $(\mathbb{Z}/n\mathbb{Z})^*$ tel que $\zeta^\sigma = \zeta^s$ pour tout ζ de μ_n ; alors $\delta^\sigma = s\delta$. Cela signifie que Σ et μ_n sont isomorphes en tant que $\mathcal{G}$-modules. ∎

2.2.2. Maintenant, n désigne à nouveau l'entier $\frac{N-1}{(N-1,12)}$.

THEOREME. Il existe un sous-groupe de J , isomorphe à μ_n sur $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

▪ D'après ce qui précède, il suffit de trouver une courbe Z définie sur $\mathbb{Q}$, non singulière, et un revêtement $\pi : Z \to X$, rationnel sur $\mathbb{Q}$, tels que l'extension $\mathbb{Q}(Z)/\mathbb{Q}(X)$ soit cyclique de degré n , non ramifiée. Considérons le recouvrement $X_1(N) \to X$, défini en dehors des pointes par : $(E,P) \to (E,\langle P\rangle)$ (voir en (I,5.4.5) la définition de $X_1(N)$) , il est rationnel sur $\mathbb{Q}$ (cf.[27]). Le degré de ce recouvrement est l'indice $[\Gamma_o(N) : \Gamma_1(N)]$, or $\Gamma_o(N)/\Gamma_1(N)$ est isomorphe à $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$ par l'application qui associe à $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, la classe de d dans $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$. Ainsi, le degré est $\frac{N-1}{2}$.

Montrons qu'il n'y a pas de ramification aux pointes : nous avons vu qu'il suffit, au voisinage des pointes, de regarder les courbes de Tate $E(q)$. Sur $X_o(N)$, au voisinage de l'infini nous devons regarder les couples $(E(q),\mu_N)$, et au voisinage de la pointe 0 , les couples $(E(q^N),\langle q\rangle/q^{N\mathbb{Z}})$ (cf. I,5.4.6). Or, au-dessus de $(E(q),\mu_N)$ on trouve les couples $(E(q),\zeta^s)$ de $X_1(N)$ où ζ est une racine primitive N-ème de l'unité fixée et où s parcourt $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$. Ainsi, il y a $\frac{N-1}{2}$ pointes de $X_1(N)$ au-dessus de la pointe ∞ de X . Et au-dessus de $(E(q^N),\langle q\rangle/q^{N\mathbb{Z}})$ on trouve les couples $(E(q^N),q^a)$, où a parcourt $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$: il y a encore $\frac{N-1}{2}$ pointes de $X_1(N)$ au-dessus de la pointe 0 de X . Et comme $\frac{N-1}{2}$ est le degré du revêtement, il n'y a pas de ramification aux pointes.

En dehors des pointes : au-dessus du point $(E,\langle P\rangle)$ de $Y_o(N)$ se trouvent les points (E,aP) de $Y_1(N)$, où a parcourt $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$. Et il y a ramification au-dessus de $(E,\langle P\rangle)$ si et seulement si il existe un entier a , différent de 1 dans $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$, tel que $(E,P) = (E,aP)$ dans $Y_1(N)$; c'est-à-dire tel que $\varepsilon P = \pm aP$ pour un automorphisme ε de E . En général, $\mathrm{Aut}\, E \simeq \mu_2$, donc $\varepsilon = \pm 1$ et il n'y a pas de ramification.

Cependant, on a $\mathrm{Aut}\, E \simeq \mu_4$ lorsque $E \simeq \mathbb{C}/\mathbb{Z}i\oplus\mathbb{Z}$. Pour que $(\mathbb{Z}/N\mathbb{Z})^*$ contienne des racines 4-èmes de l'unité autres que ± 1 , il faut et il suffit que 4 divise $N-1$, c'est-à-dire que l'on ait : $N \equiv 1 \pmod 4$.

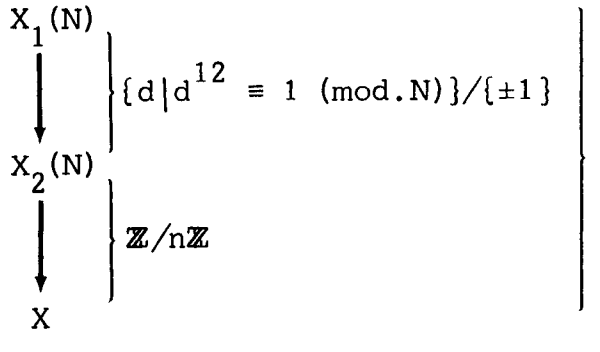
De façon analogue, $\mathrm{Aut}\, E \simeq \mu_6$ lorsque $E \simeq \mathbb{C}/\mathbb{Z}\rho\oplus\mathbb{Z}$, c'est-à-dire lorsque $N \equiv 1 \pmod 6$.

En résumé, les seuls points de $X = \overbrace{\overline{\Gamma}_o(N)\backslash\mathcal{H}}$ ramifiés dans le recouvrement $X_1(N) \to X$ sont : les conjugués de $i \pmod{\overline{\Gamma}}$ si $N \equiv 1 \pmod 4$, et leur indice est 2 ; et les conjugués de $\rho \pmod{\overline{\Gamma}}$ si $N \equiv 1 \pmod 6$, avec l'indice 3 . Lorsque $N \equiv 1 \pmod{12}$, tous les conjugués de i et $\rho \pmod{\overline{\Gamma}}$ sont ramifiés.

Remarquons que N étant un nombre premier impair, $N-1$ est pair et $n = \dfrac{N-1}{(12,N-1)}$ divise $\dfrac{N-1}{2}$.

Si $N \not\equiv 1 \pmod 4$ et $N \not\equiv 1 \pmod 6$, on a $n = \dfrac{N-1}{2}$, et le recouvrement $X_1(N) \to X$ est non ramifié cyclique de degré n .

Si $N \equiv 1 \pmod 4$ ou $N \equiv 1 \pmod 6$, le recouvrement $X_1(N) \to X$ se décompose en 2 recouvrements : $X_1(N) \to X_2(N) \to X$ si l'on définit $X_2(N)$ comme le quotient de $X_1(N)$ par les relations : $(E,P) = (E,dP)$ lorsque $d^{12} \equiv 1 \pmod N$. Cela revient à poser $X_2(N) = \overbrace{\overline{\Gamma_2(N)}\backslash\mathcal{H}}$ en définissant $\Gamma_2(N)$ comme l'image réciproque dans $\Gamma_o(N)$ du sous-groupe maximal de $\Gamma_o(N)/\Gamma_1(N)$ annulé par 12 .



Le diagramme ci-contre indique les groupes de Galois de ces revêtements.

Dans cette décomposition, le revêtement $X_2(N) \to X$ est non ramifié, cyclique de degré n .

Ainsi, la proposition (2.2.1) prouve le théorème. ∎

Ce sous-groupe de J est noté Σ est appelé <u>groupe de Shimura</u>.

2.2.3. Nous venons d'exhiber 2 sous-groupes C et Σ de J, cycliques d'ordre n. L'action de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ étant triviale sur C, et sur Σ analogue à l'action sur μ_n, l'intersection de C et Σ est réduite à 0, sauf éventuellement lorsque n est pair : dans ce cas, elle peut être d'ordre 2. En fait, nous avons le résultat suivant :

PROPOSITION. <u>Si</u> n <u>est pair</u>, $C \cap \Sigma$ <u>est d'ordre</u> 2.

■ Remarquons que n est pair si et seulement si $N \equiv 1 \pmod 8$. Nous avons vu en (2.1.4) que la fonction $g = (\frac{\Delta}{\Delta_N})^{\frac{n}{N-1}} = (\frac{\eta}{\eta_N})^{\frac{24}{(12,N-1)}}$ est dans $\mathbb{Q}(X)$, et de diviseur $n((0)-(\infty))$. Or, ici, $(12,N-1)$ est divisible par 4, donc $\frac{24}{(12,N-1)} = 2 \times \frac{3}{(3,N-1)}$. Le sous-groupe d'ordre 2 de C est engendré par $\frac{n}{2}((0)-(\infty))$ dans $J(\mathbb{Q})$; or $g^{1/2} = (\frac{\eta}{\eta_N})^{\frac{3}{(3,N-1)}}$ est une forme modulaire de type $(0,N,(\frac{\cdot}{N}))$ d'après la proposition (2.1.2), et le fait que $\frac{3}{(3,N-1)}$ est impair.

D'autre part, Σ a été obtenu à partir de l'extension $\mathbb{Q}_n(X_2(N))/\mathbb{Q}_n(X)$, par la théorie de Kummer. Posons

$$\Gamma_3(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_o(N) / (\tfrac{d}{N}) = +1\} ;$$

alors $\Gamma_3(N)$ contient $\Gamma_2(N)$, et en posant $X_3(N) = \overline{\Gamma_3(N) \backslash \mathcal{H}}$, on peut considérer les revêtements :

$$X_2(N) \longrightarrow X_3(N) \longrightarrow X_o(N) = X .$$

Or $g^{1/2}$ est une fonction sur $X_3(N)$, donc l'extension quadratique $\mathbb{Q}_n(X_3(N))/\mathbb{Q}_n(X)$ est engendrée par $g^{1/2}$; c'est une sous-extension de l'extension $\mathbb{Q}_n(X_2(N)/\mathbb{Q}_n(X)$, qui est engendrée par h : cette dernière est cyclique de degré pair, elle a donc une seule sous-extension quadratique, à savoir $\mathbb{Q}_n(X)(h^{n/2})/\mathbb{Q}_n(X)$; et d'après la théorie de Kummer (cf.[16a], 8.8) les sous-groupes $h^n.\mathbb{Q}_n(X)^{*2}$ et $g.\mathbb{Q}_n(X)^{*2}$ de $\mathbb{Q}_n(X)^*$ coïncident. Ceci

Ceci prouve que les diviseurs $\frac{n}{2}(h)$ et $\frac{1}{2}(g)$ sont linéairement équivalents. Comme leurs images dans J engendrent respectivement le sous-groupe d'ordre 2 de Σ et celui de C, la proposition est démontrée. ■

2.3. ACTION DE L'ALGEBRE DE HECKE SUR C ET Σ.

Nous avons défini en (II.2) et (II.3) les correspondances de Hecke et l'involution d'Atkin-Lehner sur X ; et nous avons montré en (II.4.2) que ces correspondances définissent des endomorphismes de J. Nous étudions ici l'action de T_ℓ (où ℓ est un nombre premier différent de N) et de $W = W_N$ sur les sous-groupes C et Σ de J.

2.3.1. *PROPOSITION*. L'homomorphisme W (resp. T_ℓ) agit sur C comme (-1) (resp. comme $(\ell+1)$).

■ (i) Rappelons que W échange les 2 pointes 0 et ∞ ; ainsi, $W((0)-(\infty)) = (\infty)-(0)$, et $(W+1)(C) = 0$.

(ii) D'autre part,

$$T_\ell((0)-(\infty)) = \left[(\ell 0) + \sum_{k=0}^{\ell-1} \left(\frac{0+k}{\ell}\right)\right] + \left[(\ell\infty) + \sum_{k=0}^{\ell-1} \left(\frac{\infty+k}{\ell}\right)\right]$$

$$= 2(0) + \sum_{k=1}^{\ell-1} \left(\frac{k}{\ell}\right) + (\ell+1)(\infty) .$$

Or kN est premier à ℓ lorsque $1 \le k \le \ell-1$, donc il existe des entiers a et b tels que $akN + b\ell = 1$; mais alors, la matrice $\begin{pmatrix} b & k \\ -Na & \ell \end{pmatrix}$ est dans $\Gamma_0(N)$ et envoie 0 sur k/ℓ ; donc $k/\ell = 0$ dans X, et $(T_\ell - (\ell+1))(C) = 0$. ■

2.3.2. *PROPOSITION*. L'homomorphisme W (resp. T_ℓ) agit sur Σ comme (-1) (resp. comme $(\ell+1)$).

■ (i) Nous avons vu, dans la démonstration de (2.2.1) et (2.2.2), que l'application : $\alpha \mapsto \frac{\alpha(h)}{h}$ définit un isomorphisme de

$G = \mathrm{Gal}(\Phi_n(X_2(N))/\Phi_n(X))$ sur μ_n ; notons ϵ cet isomorphisme. Comme $\Phi_n(X_2(N))$ est contenu dans $\Phi_n(X_1(N))$, le groupe G est un quotient de $\Gamma_o(N)/\Gamma_1(N)$; ce dernier groupe est isomorphe à $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$ par l'isomorphisme induit de : $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to d$. Considérons un élément α de G , et un représentant $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de α dans $\Gamma_o(N)$; notons $\epsilon(\gamma) = \epsilon(\alpha)$, c'est-à-dire $\epsilon(\gamma) = \frac{h \circ \gamma}{h}$; nous venons de montrer que $\epsilon(\gamma)$ ne dépend que de la classe de d dans $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$.

(ii) Rappelons que W normalise $\Gamma_o(N)$ (cf.II,1.1.2), et plus précisément, que $W \circ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ W^{-1} = \begin{pmatrix} d & -c/N \\ -Nb & a \end{pmatrix}$; comme $ad \equiv 1 \pmod{N}$, nous obtenons : $\epsilon(W.\gamma.W^{-1}) = \epsilon(\gamma)^{-1}$. Montrons que $(1+W)\delta = 0$, c'est-à-dire que $(1+W)(h)$ est le diviseur d'une fonction sur X : comme $(1+W)(h)$ est le diviseur de la fonction $h^{1+W} = h.(h \circ W)$ sur $X_2(N)$, il suffit de vérifier que $h^{1+W} \circ \gamma = h^{1+W}$ pour tout γ dans $\Gamma_o(N)$. Or $h^{1+W} \circ \gamma = (h \circ \gamma).(h \circ W \circ \gamma) = (\epsilon(\gamma)h) \cdot (\epsilon(W \circ \gamma \circ W^{-1}).h \circ W) = h^{1+W}$. Ainsi, $(1+W)(\Sigma) = 0$.

(iii) Nous voulons montrer que $D_\ell = (T_\ell - (\ell+1))(D)$ est le diviseur d'une fonction sur X , lorsque D est le diviseur défini par : $(f) = nD$ (rappelons que la fonction $f = h^n$ a été introduite en 2.2). Or $n.D_\ell = (T_\ell - (\ell+1))((f)) = T_\ell((f)) - (f^{\ell+1})$, et nous avons vu en (II,4.2) que $T_\ell((f))$ est le diviseur de la fonction (notée $f \mid T_\ell$) définie de la manière suivante (cf.II,2.2.2) : on note

$$\Sigma_\ell = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})/ad-bc = \ell \ , \ c \equiv 0 (\mathrm{mod}.N) \ , \ (a,N) = 1 \right\}$$

(ce groupe Σ_ℓ n'yant rien à voir avec le groupe de Shimura Σ) ; $\{\alpha_i\}_{1 \le i \le \ell+1}$ un système (quelconque) de représentants des classes à gauche de Σ_ℓ modulo $\Gamma_o(N)$; et alors $f \mid T_\ell = \prod_{i=1}^{\ell+1} f \circ \alpha_i^{-1}$. Par exemple, on peut choisir $\{\alpha_i\}_{1 \le i \le \ell+1} = \{\begin{pmatrix} 1 & b \\ 0 & \ell \end{pmatrix}\}_{0 \le b < \ell} \cup \{\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}\}$.

De façon analogue, notons

$$\Sigma'_\ell = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})/ab-bc = \ell \ , \ c \equiv 0(\mathrm{mod}.N) \ , \ a \equiv 1(\mathrm{mod}.N) \right\} \ ;$$

$\{\alpha'_i\}_{1\le i\le \ell+1}$ un système (quelconque) de représentants des classes à gauche de Σ'_ℓ modulo $\Gamma_1(N)$; et $h \mid T_\ell = \prod_{i=1}^{\ell+1} h\circ\alpha_i'^{-1}$ (rappelons que h est une fonction sur $X_1(N)$) . Cette définition est justifiée dans ([43].3). Mais on peut choisir $\{\alpha_i\}_{1\le i\le \ell+1} = \{\alpha'_i\}_{1\le i\le \ell+1} = \{\begin{pmatrix}1 & b\\ 0 & \ell\end{pmatrix}\}_{0\le b<\ell} \cup \{\begin{pmatrix}\ell a & b\\ N\ell & \ell\end{pmatrix}\}$, où a et b sont tels que : $\ell a - Nb = 1$ (rappelons que N est premier à ℓ) ; en effet, $\begin{pmatrix}\ell a & b\\ N\ell & \ell\end{pmatrix} = \begin{pmatrix}a & b\\ N & \ell\end{pmatrix}\begin{pmatrix}\ell & 0\\ 0 & 1\end{pmatrix}$ et $\begin{pmatrix}a & b\\ N & \ell\end{pmatrix} \in \Gamma_o(N)$. Cela prouve que

$$(h \mid T_\ell)^n = h^n \mid T_\ell = f \mid T_\ell .$$

En résumé, D_ℓ est le diviseur de la fonction $\dfrac{h \mid T_\ell}{h^{\ell+1}}$ sur $X_2(N)$; nous allons voir qu'en fait, cette fonction est définie sur X : soit γ un élément de $\Gamma_o(N)$; alors $h^{\ell+1}\circ\gamma = \varepsilon(\gamma)^{\ell+1}h$, et d'autre part $(h \mid T_\ell)\circ\gamma = (\prod_{i=1}^{\ell+1} h\circ\alpha_i'^{-1})\circ\gamma = \prod_{i=1}^{\ell+1} h\circ\gamma\circ\alpha_i''^{-1} = \varepsilon(\gamma)^{\ell+1}\prod_{i=1}^{\ell+1} h\circ\alpha_i''^{-1}$ si $\alpha_i'' = \gamma^{-1}\circ\alpha'_i\circ\gamma$; or $\{\alpha_i''\}_{1\le i\le \ell+1}$ forme, comme $\{\alpha'_i\}_{1\le i\le \ell+1}$, un système de représentants à gauche de Σ'_ℓ modulo $\Gamma_1(N)$; donc $(h \mid T_\ell)\circ\gamma = \varepsilon(\gamma)^{\ell+1}(h \mid T_\ell)$,et $\dfrac{h \mid T_\ell}{h^{\ell+1}}$ est une fonction sur X . ∎

2.3.3. Les groupes C et Σ sont-ils contenus dans $J_- = (1-W)J$? Nous avons le résultat suivant :

LEMME .

(i) Pour tout point P de X , l'image du diviseur $(P) - (WP)$ dans J est en fait dans J_- ;

(ii) Si x désigne un point de J d'ordre fini impair, sur lequel W agit comme (-1) , alors x est dans J_- ;

(iii) Le groupe "parabolique" C et la composante 2-primaire du groupe de Shimura Σ sont des sous-groupes de J_- .

∎ On note ici de la même manière les diviseurs de degré nul sur X et leurs images dans J .

(i) D'après (1.2.3), il existe toujours au moins un point de X fixe par W ; notons Q un tel point. Alors $(P)-(WP) = (1-W)((P)-(Q))$ est bien dans J_-. En particulier, lorsque $P = 0$, on a : $WP = \infty$, donc le générateur $(0)-(\infty)$ de C est dans J_- ; ainsi, C est un sous-groupe de J_-.

(ii) D'une part $2x = (1-W)x$ est dans J_- ; et d'autre part mx est nul pour un nombre impair m, donc $x = m'.2x$, si m' désigne un entier inverse de 2 modulo m. Ainsi, x est dans J_-. En particulier, ceci s'applique à tous les points de la composante 2-primaire de Σ. ∎

Désormais, nous appelons <u>algèbre de Hecke</u>, et notons $\mathbb{H}$, la sous-algèbre de $\mathrm{End}(J)$ engendrée par les opérateurs de Hecke T_ℓ (pour tout nombre premier ℓ différent de N), et par l'opérateur d'Atkin-Lehner W. Nous appelons <u>idéal d'Eisenstein</u>, et notons <u>Eis</u>, l'idéal de $\mathbb{H}$ engendré par les opérateurs : $T_\ell-(\ell+1)$ et $W+1$.

Ce qui précède se résume dans la proposition suivante :

<u>Résumé</u>. <u>La variété</u> J <u>possède deux sous-groupes cycliques</u> C <u>et</u> Σ, <u>d'ordre</u> n, <u>rationnels sur</u> $\mathbb{Q}$, <u>annulés par</u> Eis ; <u>de plus</u>, <u>tous les points de</u> C <u>sont rationnels sur</u> $\mathbb{Q}$, <u>alors que</u> $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ <u>agit sur</u> Σ "<u>comme sur</u>" μ_n ; <u>l'intersection de</u> C <u>et</u> Σ <u>est triviale si</u> n <u>est impair</u>, <u>d'ordre</u> 2 <u>si</u> n <u>est pair</u> ; <u>enfin</u>, C <u>et la composante 2-primaire de</u> Σ <u>sont contenus dans</u> $J_- = (1-W)J$.

2.4. <u>LOCALISATION DE L'ALGEBRE DE HECKE</u>.

2.4.1. Notons I l'idéal $(n,\underline{\mathrm{Eis}})$.

LEMME. <u>L'homomorphisme de</u> $\mathbb{H}$ <u>dans</u> C <u>défini par</u> : $T \mapsto T((0)-(\infty))$ <u>induit un isomorphisme d'anneaux entre</u> $\mathbb{H}/I$ <u>et</u> $\mathbb{Z}/n\mathbb{Z}$.

■ On vérifie immédiatement que cette application est un homomorphisme d'anneaux. Comme l'image de 1 est un générateur de C, cet homomorphisme est surjectif. Le noyau contient n car $n((0)-(\infty)) = 0$, et il contient $\underline{\text{Eis}}$ d'après (2.3.4) ; d'où un homomorphisme φ de $\mathbb{H}/I$ sur C.

D'autre part, l'homomorphisme canonique de $\mathbb{Z}$ dans $\mathbb{H}/\underline{\text{Eis}}$ (composé de l'injection de $\mathbb{Z}$ dans $\mathbb{H}$ et de la projection de $\mathbb{H}$ sur $\mathbb{H}/\underline{\text{Eis}}$) induit un homomorphisme ψ de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{H}/I$.

Enfin, le composé : $\mathbb{H}/I \xrightarrow{\varphi} C \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z} \xrightarrow{\psi} \mathbb{H}/I$ est l'identité (c'est immédiat sur les générateurs T_ℓ et W de $\mathbb{H}$). ■

Remarque : Mazur a montré [21] que n est contenu dans Eis, autrement dit que $I = \underline{\text{Eis}}$ et que $\mathbb{H}/\underline{\text{Eis}}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

2.4.2. Notons p un facteur premier IMPAIR de n ; P l'idéal de $\mathbb{H}$ engendré par $\underline{\text{Eis}}$ et p ; d'après le lemme (2.4.1), $\mathbb{H}/P$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, donc P est un idéal maximal de $\mathbb{H}$.

Notons $\mathbb{H}_p = \varprojlim_m \mathbb{H}/p^m\mathbb{H}$ (resp. $\mathbb{H}_P = \varprojlim_m \mathbb{H}/P^m$) le complété p-adique (resp. P-adique) de $\mathbb{H}$.

Rappelons que g désigne de genre de X, c'est-à-dire la dimension de J (cf.II,4.1.2).

PROPOSITION.

(i) $\mathbb{H}$ est un $\mathbb{Z}$-module libre de rang g ;

(ii) $\mathbb{H}_p$ est un $\mathbb{Z}_p$-module libre de rang g ;

(iii) $\mathbb{H}_P$ est facteur direct de $\mathbb{H}_p$ en tant qu'anneau.

■ (i) Il est clair que $\mathbb{H}$ est un $\mathbb{Z}$-module de type fini sans torsion, donc libre. L'action des opérateurs de Hecke et d'Atkin-Lehner sur les formes différentielles holomorphes sur J permet de définir un homomorphisme injectif de $\mathbb{H}$ dans l'anneau des endomorphismes de ces formes

différentielles. Cela signifie (cf.II,4.1.5) que l'homomorphisme canonique de $\mathbb{H}$ dans l'anneau des endomorphismes de l'espace $S(2,N)$ (espace des formes paraboliques de poids 2 pour $\Gamma_0(N)$) est injectif. Il suffit donc de montrer que l'image de $\mathbb{H}$ (encore notée $\mathbb{H}$) par cet homomorphisme a un $\mathbb{Z}$-rang égal à g . Le $\mathbb{C}$-espace vectoriel $S(2,N)$ est de dimension g (cf.II,4.1.5) et on peut montrer qu'il contient un réseau (de rang $2g$) stable par $\mathbb{H}$ (cf.[43], (3.5.20)). Considérons une base de ce réseau ; elle comporte $2g$ éléments et forme une base de $S(2,N)$ sur $\mathbb{R}$. Dans cette base, les éléments de $\mathbb{H}$ sont représentés par des matrices à coefficients entiers, donc $\mathbb{H}$ est inclus dans l'espace $M_{2g}(\mathbb{Z})$ des matrices carrées d'ordre $2g$ à coefficients entiers. Ainsi, $\mathbb{H}$ est un $\mathbb{Z}$-module libre de rang fini m $(m \leq 4g^2)$ et m est la dimension sur $\mathbb{C}$ de $\mathbb{H} \otimes_{\mathbb{Z}} \mathbb{C}$.

Comme N est premier, toutes les formes de $S(2,N)$ sont primitives (cf.II,3.3.5), et il existe une base de $S(2,N)$ formée de fonctions propres pour tous les éléments de $\mathbb{H}$ (cf.II,3.3.4) : d'où $m \leq g$. De plus, les valeurs propres d'une fonction propre pour tous les éléments de $\mathbb{H}$ déterminent la fonction propre (à un coefficient près) (cf.II,2.3.1) , donc on a exactement : $m = g$.

(ii) Comme $\mathbb{H}_p$ est isomorphe à $\mathbb{H} \otimes_{\mathbb{Z}} \mathbb{Z}_p$, l'assertion (ii) résulte immédiatement de (i) .

(iii) Les projections canoniques de $\mathbb{H}/p^m\mathbb{H}$ sur $\mathbb{H}/P^m$ forment un système compatible avec les systèmes projectifs $\{\mathbb{H}/p^m\mathbb{H}\}$ et $\{\mathbb{H}/P^m\}$, et induisent donc une projection canonique de $\mathbb{H}_p$ sur $\mathbb{H}_P$.

D'autre part, pour tout entier $m \geq 1$, l'anneau $\mathbb{H}/p^m\mathbb{H}$ est artinien ; il est donc produit direct de ses composantes locales. Par passage à la limite, l'anneau proartinien $\mathbb{H}_p$ est produit direct de ses composantes locales, donc $\mathbb{H}_P$ est facteur direct de $\mathbb{H}_p$. ∎

3. *POINTS D'ORDRE FINI DE J .*

3.1. SCHEMA DE NERON DE J .

3.1.1. Soit K un corps de nombres, d'anneau des entiers S . Rappelons que J désigne la jacobienne de $X_0(N)$. Nous pouvons attacher à la variété abélienne J (définie sur $\mathbb{Q}$, donc sur K) son schéma de Néron sur S (cf.[24] ,[42] ,[20]) , noté ici J_S . La fibre de ce schéma au-dessus du point générique 0 de Spec S est J(K) ; au-dessus d'un point $\mathfrak{p}$ de bonne réduction pour J (i.e. $\mathfrak{p}$ ne divise pas N) , la fibre est la réduction de J modulo $\mathfrak{p}$; enfin, au-dessus d'un point $\mathfrak{p}$ divisant N , la fibre est "de type multiplicatif", comme le montre le théorème de Deligne énoncé ci-dessous (3.1.2).

La composante connexe de l'élément neutre de ce schéma de Néron est un schéma sur S , appelé composante connexe de J_S et noté J_S^c .

On note $J_{/\mathfrak{p}}$ (resp. $J^c_{/\mathfrak{p}}$) la fibre en $\mathfrak{p}$ de J_S (resp. de J_S^c). Si $\mathfrak{p}$ ne divise pas N , alors $J^c_{/\mathfrak{p}}$ et $J_{/\mathfrak{p}}$ coïncident.

3.1.2. Deligne a démontré le résultat suivant, concernant la structure de la fibre en N du schéma de Néron de J sur $\mathbb{Q}$ (cf.[1] ,II,De-Ra).

THEOREME . La composante connexe $J^c_{/N}$ est un groupe de type multiplicatif ;

La spécialisation en N du groupe C , notée $\overline{C}$, est un groupe cyclique d'ordre n ;

La fibre $J_{/N}$ est égale au produit : $J^c_{/N} \times \overline{C}$;

Le Frobenius π_N agit sur $J^c_{/N}$ comme (-NW) , et sur $\overline{C}$ comme (-1) .

Nous indiquerons en (5.1) comment on peut montrer que $J_{/N}$ est isomorphe à $J^c_{/N} \times \overline{C}$.

3.1.3. Une conséquence de ce théorème est le résultat suivant :

COROLLAIRE. Le groupe C est facteur direct dans $J(\mathbb{Q})$.

■ Comme C et $\overline{C}$ ont même ordre n , la spécialisation en N , restreinte à C , admet une application réciproque (de $\overline{C}$ dans C). En composant : la spécialisation en N (de $J(\mathbb{Q})$ dans $J_{/N}$) , la projection canonique (de $J_{/N}$ sur C) , et cette application réciproque de la spécialisation (de $\overline{C}$ dans C) , on définit une rétraction de $J(\mathbb{Q})$ sur C . ■

Nous verrons en (3.2.4) que C est le groupe de torsion de $J(\mathbb{Q})$.

3.2. NOYAU DE P DANS $J(\mathbb{Q})$ ET GROUPE DE TORSION DE $J(\mathbb{Q})$.

3.2.1. Pour l'instant, notons p un nombre premier quelconque. On appelle sous-groupe de type $\mathbb{Z}/p\mathbb{Z}$ (resp. de type μ_p) de J tout sous-groupe cyclique d'ordre p de J sur lequel $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ agit trivialement (resp. agit comme sur les racines p-èmes de l'unité dans $\overline{\mathbb{Q}}$). Rappelons que le noyau de la multiplication par p dans C (resp. dans Σ) est nul si p ne divise pas n , et que c'est un sous-groupe de type $\mathbb{Z}/p\mathbb{Z}$ (resp. de type μ_p) , noté C_p (resp. Σ_p) si p divise n . Rappelons aussi que C et Σ sont annulés par l'idéal d'Eisenstein Eis (cf.2.3).

PROPOSITION. Si p est un nombre premier impair, alors tout sous-groupe de J de type $\mathbb{Z}/p\mathbb{Z}$ où μ_p est annulé par l'idéal d'Eisenstein.

■ A tout sous-groupe de type $\mathbb{Z}/p\mathbb{Z}$ (resp. μ_p) de J est associé un sous-schéma du schéma de Néron $J_{\mathbb{Z}}$ de J sur $\mathbb{Z}$.

Etudions d'abord l'action de T_ℓ (pour $\ell \neq N$) sur $\mathbb{Z}/p\mathbb{Z}$. Si p est différent de N, le groupe des points de J annulés par p et rationnels sur $\mathbb{Q}$ s'identifie au groupe des points définis sur $\mathbb{Z}$ dans le schéma en groupes $J_{\mathbb{Z}}[p]$ (noyau de p dans $J_{\mathbb{Z}}$). Notons $J_{\mathbb{Z}_\ell}[p]$ le schéma en groupes obtenu à partir de $J_{\mathbb{Z}}[p]$ en étendant les scalaires à $\mathbb{Z}_\ell$. Comme $\ell \neq N$, $J_{\mathbb{Z}_\ell}[p]$ est un schéma en groupes fini et plat de type $p,p,\ldots,p)$ sur l'anneau local $\mathbb{Z}_\ell$. Or le foncteur qui, à un schéma en groupes G fini et plat de type $(p,p,\ldots,p)$ sur $\mathbb{Z}_\ell$, associe le schéma en groupes $G \otimes_{\mathbb{Z}_\ell} \mathbb{F}_\ell$ sur $\mathbb{F}_\ell$ est pleinement fidèle, sauf si $\ell = p = 2$ (lorsque $\ell \neq p$, c'est même une équivalence de catégorie) (cf.[8a], démonstration du théorème 2, première étape). Ainsi, l'homomorphisme de réduction modulo ℓ, restreint aux points de $J_{\mathbb{Z}}[p]$ définis sur $\mathbb{Z}$, est injectif.

Etudions l'action de T_ℓ en réduction modulo ℓ, en utilisant la formule d'Eichler Shimura : $\tilde{T}_\ell = \pi_\ell + \pi'_\ell$ (cf.II,7.2), ainsi que la formule : $\pi_\ell \cdot \pi'_\ell = \pi'_\ell \cdot \pi_\ell = \ell$. Sur $\mathbb{Z}/p\mathbb{Z}$, π_ℓ agit comme l'identité, dans π'_ℓ comme ℓ et $\tilde{T}_\ell$ comme $1+\ell$. Soit x un point de $\mathbb{Z}/p\mathbb{Z}$; alors $(T_\ell - (1+\ell))(x)$ est dans $\mathbb{Z}/p\mathbb{Z}$, et sa réduction modulo ℓ est nulle. D'après ce qui précède, ceci implique que $(T_\ell-(1+\ell))(x)$ est nul.

Un raisonnement analogue prouve que $(T_\ell-(1+\ell))(x)$ (pour $\ell \neq N$) est nul si x est dans μ_p et $p \neq N$: il suffit de remplacer $\mathbb{Q}$ par $\mathbb{Q}(\sqrt[p]{1})$, $\mathbb{Z}_\ell$ par l'anneau $\mathcal{O}$ des entiers de $\mathbb{Q}_\ell(\sqrt[p]{1})$, $\mathbb{F}_\ell$ par $\mathcal{O}/\ell\mathcal{O}$, pour se ramener à l'étude modulo ℓ. Ensuite, on remarque que π_ℓ agit sur μ_p comme ℓ, donc π'_ℓ comme 1 et $\tilde{T}_\ell$ comme $\ell+1$.

Pour montrer que $T_\ell-(\ell+1)$ (pour $\ell \neq N$) annule $\mathbb{Z}/N\mathbb{Z}$ et μ_N, voir [21].

Pour étudier l'action de W, on peut montrer (cela fait partie des "bonnes propriétés" du schéma de Néron), qu'il suffit de façon analogue, d'étudier l'action de W sur la fibre en N du schéma de Néron de J. D'après le théorème (3.1.2), on a : $J_{/N} = \overline{C} \times J^c_{/N}$; pour montrer que W agit comme (-1) sur tout sous-groupe de type $\mathbb{Z}/p\mathbb{Z}$ ou μ_p de $J_{/N}$,

il suffit de montrer que W agit comme (-1) sur tout sous-groupe de type $\mathbb{Z}/p\mathbb{Z}$ ou μ_p de $\overline{C}$ ou de J^c/N . Comme $\overline{C}$ n'a pas de sous-groupe de type μ_p , trois cas sont à considérer :

- Le cas d'un sous-groupe de type $\mathbb{Z}/p\mathbb{Z}$ de $\overline{C}$: il est annulé par $W+1$, comme $\overline{C}$ (d'après 3.1.2) .

- Le cas d'un sous-groupe de type $\mathbb{Z}/p\mathbb{Z}$ de J^c/N : d'après (3.1.2), J^c/N est un groupe de type multiplicatif, donc $J^c/N\,(\mathbb{F}_N)$ est un sous-groupe d'un produit de $\mathbb{F}_N^*$; ainsi, tout élément de torsion de $J^c/N\,(\mathbb{F}_N)$ est d'ordre divisant $(N-1)$. En particulier, s'il existe un sous-groupe de type $\mathbb{Z}/p\mathbb{Z}$ de J^c/N , alors p divise $(N-1)$; cela prouve que W agit sur $\mathbb{Z}/p\mathbb{Z}$ comme NW , donc comme $(-\pi_N)$ (d'après 3.1.2), c'est-à-dire comme (-1) .

- Le cas d'un sous-groupe de type μ_p de J^c/N : si un tel sous-groupe existe, alors p est différent de N ; or π_N agit sur μ_p comme N , donc $N(W+1)$ comme $(NW+\pi_N)$, or $(NW+\pi_N)$ annule μ_p d'après (3.1.2) . Ainsi, $N(W+1)$ annule μ_p , et comme p est différent de N , on voit que $W+1$ annule μ_p . ∎

3.2.2. D'autre part, notons Z une courbe non singulière définie sur un corps parfait de caractéristique $p > 0$; notons $J(Z)$ la jacobienne de Z , $J(Z)_p$ le noyau de la multiplication par p dans $J(Z)$, et $\mathrm{Dif}_o(Z)$ l'espace des formes différentielles holomorphes sur Z . Le résultat suivant est dû à Hasse :

LEMME. Il existe un homomorphisme de groupes injectif de $J(Z)_p$ dans $\mathrm{Dif}_o(Z)$.

∎ Soit D un diviseur de degré nul sur Z , tel que $p.D$ soit le diviseur d'une fonction f sur Z : autrement dit, l'image $\overline{D}$ de D dans $J(Z)$ est d'ordre divisant p . Considérons la forme différentielle $\frac{df}{f}$ sur Z , et montrons qu'elle est holomorphe : soient Q un point de Z , t un paramètre local en Q , tel que $f(t) = t^\alpha + a_1 t^{\alpha+1} + \ldots$ soit la va-

leur de f dans un voisinage de Q ; comme le diviseur de f est un multiple de p, l'ordre α de f en Q est divisible par p, et $\frac{df}{f} = \frac{(\alpha+1)a_1 t^{\alpha}+\ldots}{t^{\alpha}+\ldots} dt$ est une série entière en t ; ainsi, $\frac{df}{f}$ est holomorphe en tout point Q de Z ; autrement dit, $\frac{df}{f}$ est dans $\mathrm{Dif}_o(Z)$. Si D est lui-même le diviseur d'une fonction g, alors $f = g^p$, et $\frac{df}{f} = p\frac{dg}{g} = 0$. Donc on définit une application de $J(Z)_p$ dans $\mathrm{Dif}_o(Z)$ en faisant correspondre à $\overline{D}$ la forme $\frac{df}{f}$. Cette application est un homomorphisme (la vérification est immédiate), et nous allons montrer qu'il est injectif : si $\frac{df}{f}$ est nul, c'est-à-dire si $df = 0$, alors f est défini, au voisinage de tout point Q de Z, par une série entière en t^p ; donc f est une puissance p-ème au voisinage de tout point de Z, ce qui montre que f est de la forme g^p sur Z, et que $\overline{D} = \overline{(g)} = 0$. ∎

3.2.3. Nous pouvons maintenant énoncer le résultat fondamental, dû à Mazur, Serre et Katz [21]. Soit p un nombre premier impair ; on note P l'idéal de $\mathbb{H}$ engendré par $\underline{\mathrm{Eis}}$ et p, et $J(\mathbb{Q})_P$ le groupe des points de $J(\mathbb{Q})$ annulés par P. Rappelons que $J(\mathbb{Q})_p$ (resp. C_p) désigne le noyau de la multiplication par p dans $J(\mathbb{Q})$ (resp. dans C). On a les inclusions : $C_p \subset J(\mathbb{Q})_P \subset J(\mathbb{Q})_p$ (cf.2.3.1), et l'on sait que C_p est trivial si p ne divise pas n, et isomorphe à $\mathbb{Z}/p\mathbb{Z}$ si p divise n (cf.2.1.4).

THEOREME. Les espaces C_p et $J(\mathbb{Q})_P$ sont égaux.

∎ Supposons p différent de N ; l'homomorphisme canonique de $J(\mathbb{Q})_p$ dans $J(\mathbb{F}_p)_p$ est injectif (cf [8a] et la démonstration de 3.2.1); or le lemme de Hasse (3.2.2) définit une injection de $J(\mathbb{F}_p)_p$ dans $\mathrm{Dif}_o(\tilde{X})$, si $\tilde{X}$ désigne la réduction de X modulo p ; on a ainsi une injection de $\mathbb{F}_p$-espaces vectoriels de $J(\mathbb{Q})_p$ dans $\mathrm{Dif}_o(\tilde{X})$.

Montrons que cette injection est compatible avec l'action de $\mathbb{H}$; il suffit de vérifier qu'elle est compatible avec l'action de T_ℓ pour tout nombre premier ℓ (puisque $T_N = -W$, d'après II,3.3.5). Soit donc D

un diviseur de degré nul sur X , tel que $p.D$ soit le diviseur d'une fonction f ; alors $p(T_\ell D) = T_\ell(pD) = T_\ell((f))$ est le diviseur de la fonction $f \mid T_\ell$ (cf.II,4.2.1) ; rappelons que $f \mid T_\ell$ est définie par : $f \mid T_\ell = \prod_i f \circ \alpha_i^{-1}$, si $\{\alpha_i\}_i$ forme un système quelconque de représentant de l'ensemble Σ_ℓ (qui a été défini en II,2.2.2 et n'a rien à voir avec le groupe de Simura) modulo l'action à gauche de $\Gamma_o(N)$. Ainsi,

$$\frac{d(f \mid T_\ell)}{f \mid T_\ell} = \sum_i \frac{d(f \circ \alpha_i^{-1})}{f \circ \alpha_i^{-1}} ,$$

et si l'on prend pour $\{\alpha_i\}_i$ un système de représentants à la fois à droite et à gauche de Σ_ℓ modulo $\Gamma_o(N)$ (c'est possible d'après II,3.1.3), on voit que $\frac{d(f \mid T_\ell)}{f \mid T_\ell}$ est égal à $\frac{df}{f} \mid T_\ell$. Ainsi, l'injection de $J(\mathbb{Q})_p$ dans $\mathrm{Dif}_o(\widetilde{X})$ est compatible avec l'action de $\mathbb{H}$ et définit une injection de $J(\mathbb{Q})_P$ dans $\mathrm{Dif}_o(\widetilde{X})_{\underline{\mathrm{Eis}}}$ (noyau de $\underline{\mathrm{Eis}}$ dans $\mathrm{Dif}_o(\widetilde{X})$).

En résumé, on a les injections : $C_p \subset J(\mathbb{Q})_P \subset \mathrm{Dif}_o(\widetilde{X})_{\underline{\mathrm{Eis}}}$, et la proposition suivante (3.2.4) termine la démonstration du théorème pour $p \neq N$. Pour $p = N$, voir [21] . ∎

3.2.4. (on suppose toujours p premier impair).

PROPOSITION. (Katz [1] III) <u>Le noyau de Eis dans</u> $\mathrm{Dif}_o(\widetilde{X})$ <u>est un espace vectoriel sur</u> $\mathbb{F}_p$ <u>de dimension inférieure ou égale à</u> 1 <u>lorsque</u> p <u>divise</u> n , <u>de dimension nulle sinon</u>.

∎ Nous essayons ci-dessous d'expliquer le principe de la démonstration de cette proposition, dû à Katz.

On montre d'abord que la dimension de $\mathrm{Dif}_o(\widetilde{X})_{\underline{\mathrm{Eis}}}$ sur $\mathbb{F}_p$ est au plus égale à 1 . Pour cela, admettons que l'espace $\mathrm{Dif}_o(\widetilde{X})$ est isomorphe à l'espace des "<u>formes paraboliques de poids</u> 2 <u>modulo</u> p" (cf [21], et [1] III, Katz, Serre). On peut avoir une idée naïve de ces formes en considérant les développements de Fourier des formes modulaires pour $\Gamma_o(p)$

sur $\mathcal{H}$: $f(q) = \sum_{n=0}^{\infty} a_n q^n$: si les coefficients a_n sont entiers en p, on pose $\tilde{f}(q) = \sum_{n=0}^{\infty} \tilde{a}_n q^n$ (où $\tilde{a}_n$ est la réduction modulo p de a_n), on appelle $\tilde{f}$ une forme modulaire modulo p, et on définit le poids de $\tilde{f}$ comme la classe, modulo $(p-1)$, du poids de f. Cette définition du poids est un peu justifiée par le cas des séries d'Eisenstein (cf.I,2.1.9) : si d est un entier premier à p, et si k et k' sont congrus (modulo $(p-1)$), alors $d^{k*} \equiv d^{k'}$ (modulo p), donc $E_k \equiv E_{k'}$ (mod.p). Disons qu'une forme modulaire modulo p est parabolique si son terme constant est nul. Rappelons qu'il existe une base de l'espace $S(2,p)$ des formes paraboliques de poids 2 pour $\Gamma_0(p)$, formée de vecteurs propres pour tous les opérateurs de Hecke, les valeurs propres étant proportionnelles aux coefficients de Fourier (cf.II,3.3.4 et II.3.3.5). Admettons qu'il en est de même pour l'espace des formes paraboliques de poids 2 modulo p : soit φ une forme parabolique de poids 2 modulo p, vecteur propre pour tous les opérateurs de Hecke, de développement de Fourier $\sum_{m=1}^{\infty} b_m q^m$, normalisée par : $b_1 = 1$; alors b_ℓ (pour ℓ premier) est la valeur propre de l'opérateur T_ℓ associée au vecteur propre φ, et tous les b_m sont déterminés par les b_ℓ (cf.II,2.1.3 ou II,2.3.1). Supposons que φ est annulée par $\underline{\text{Eis}}$; comme $\underline{\text{Eis}}$ est engendré par les $T_\ell - (\ell+1)$ (pour $\ell \neq N$) et par $W+1 = -T_N+1$ (cf.II,3.3.5), on a forcément $b_\ell = \ell+1$ (si $\ell \neq N$) et $b_N = 1$; d'où le développement de Fourier de φ : $\varphi(q) = \sum_{m=1}^{\infty} \sigma'_1(m) q^m$, où $\sigma'_1(m) = \sum_{\substack{d \mid m \\ (d,N)=1}} d$.

Or Katz a montré (cf [1], III) que le principe de q-développement (cf II,7.1.1) est encore valable pour les formes modulaires modulo p ; donc il existe au plus une fonction propre normalisée φ dans le noyau de $\underline{\text{Eis}}$; ceci prouve que la dimension de $\text{Dif}_0(X)_{\underline{\text{Eis}}}$ sur $\mathbb{F}_p$ est au plus égale à 1.

Montrons maintenant que cette dimension est nulle lorsque p ne divise pas n : considérons la fonction $g = \Delta_N/\Delta$ (déjà utilisée en (2.1.4), où elle était notée $1/f$). Nous avons vu que g est dans $\mathcal{Q}(X)$. Considérons sa dérivée logarithmique (par rapport à τ) : nous obtenons

$2\pi iq \frac{d}{dq} \log(g(q)) = \frac{g'(q)}{g(q)}$ en notant (abusivement) $g'(q)$ le développement de Fourier de $g'(\tau)$. D'autre part, $\Delta(q) = q.\prod_{n\geq 1} (1-q^n)^2$ donc

$$\frac{d}{dq} \log(g(q)) = \frac{N-1}{q} + 24 \sum_{n\geq 1} \sigma_1'(n) q^{n-1}$$

et

$$h(q) = \frac{1}{24} . q \frac{d}{dq} \log(g(q)) = \frac{N-1}{24} + \sum_{n\geq 1} \sigma_1'(n) q^n$$

est une forme modulaire de poids 2 pour $\Gamma_0(N)$. On vient ainsi d'exhiber une "forme modulaire de poids 2 modulo p" sur X . Si φ existe, $\tilde{h} - \varphi = \frac{N-1}{24}$ est une constante : elle doit être nulle, ce qui équivaut (lorsque $p \geq 5$) à dire que p divise n , et termine la "démonstration" de la proposition pour $p \neq 3$. En fait, pour $p = 3$, il existe encore une théorie des formes modulaires modulo 3 , qui permet de faire une démonstration analogue. ∎

3.2.4. Nous pouvons maintenant prouver le résultat suivant :

THEOREME. Le groupe de torsion de $J(\mathbb{Q})$ est égal à C .

∎ Comme d'habitude, nous démontrons seulement que les composantes 2-primaires de $J(\mathbb{Q})$ et C sont égales ; voir Mazur [21] pour l'étude des 2-composantes.

D'après (3.1.3), $J(\mathbb{Q})$ est de la forme $C \oplus D$ pour un certain sous-groupe D . Si D a de la p-torsion (pour un nombre premier impair p), cela signifie que D contient un groupe de type $\mathbb{Z}/p\mathbb{Z}$, donc que $J(\mathbb{Q})$ contient $\mathbb{Z}/p\mathbb{Z} \oplus C_p$ (où C_p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ si p divise n , nul sinon). Or tout sous-groupe de J de type $\mathbb{Z}/p\mathbb{Z}$ est annulé par l'idéal d'Eisenstein, d'après (3.2.1), donc $\mathbb{Z}/p\mathbb{Z} \oplus C_p$ est contenu dans $J(\mathbb{Q})_p$, ce qui contredit le théorème (3.2.3). ∎

3.3. NOYAU DE P DANS J .

Maintenant, p désigne un diviseur premier de n , différent de 2 , et P l'idéal (Eis,p) de $\mathbb{H}$; on note J_P le groupe des points de J annulés par P .

3.3.1. *LEMME* (cf [21]). Comme module sur $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, J_P admet une suite de Jordan-Hölder dont les quotients sont tous isomorphes à $\mathbb{Z}/p\mathbb{Z}$ ou à μ_p .

▪ Comme J_P est annulé par P , donc par Eis , on a : $T_\ell = \ell+1$ (pour tout $\ell \neq N$) et $W = -1$ sur J_P . Considérons la réduction modulo ℓ d'un quotient de Jordan-Hölder de J_P ; notons Q ce quotient et $\tilde{Q}$ sa réduction ; le Frobenius π_ℓ et son transposé π'_ℓ sur $\tilde{Q}$ vérifient : $\pi_\ell.\pi'_\ell = \ell$, et $\pi_\ell + \pi'_\ell = \tilde{T}_\ell = \ell+1$ (formule d'Eichler-Shimura) ; autrement dit, ce sont les deux racines du trinôme $X^2 - (\ell+1)X + \ell = (X-1)(X-\ell)$. Notons λ_1 (resp. λ_2) le nombre de quotients, dans une suite de Jordan-Hölder de J_P , sur lesquels $\pi_\ell = 1$ (resp. $\pi_\ell = \ell$) (remarquons que $\lambda_1+\lambda_2$ est la dimension de J_P sur $\mathbb{F}_p$) .

Considérons maintenant le module $(\mathbb{Z}/p\mathbb{Z})^{\lambda_1} \oplus \mu_p^{\lambda_2}$ sur $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, et un quotient fini G de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, assez grand pour que les opérations de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur J_P et sur $(\mathbb{Z}/p\mathbb{Z})^{\lambda_1} \oplus \mu_p^{\lambda_2}$ se factorisent par G . Soit ℓ un nombre premier non ramifié dans l'extension finie K de $\mathbb{Q}$ de groupe de Galois G , et π_ℓ l'automorphisme de Frobenius correspondant. Les valeurs propres de π_ℓ sur la réduction (mod.ℓ) de $(\mathbb{Z}/p\mathbb{Z})^{\lambda_1} \oplus \mu_p^{\lambda_2}$ sont les mêmes que les valeurs propres de π_ℓ sur la réduction (mod.ℓ) de J_P . Comme G est engendré par ces automorphismes π_ℓ , lorsque ℓ parcourt l'ensemble des nombres premiers non ramifiés dans $K/\mathbb{Q}$ (théorème de densité), on voit que les valeurs propres (et leurs multiplicités) de tout élément de G sont les mêmes pour les deux G-modules J_P et $(\mathbb{Z}/p\mathbb{Z})^{\lambda_1} \oplus \mu_p^{\lambda_2}$.

Mais alors, un théorème dû à Brauer et Nesbitt sur les représentations des groupes finis (cf [6b], 30, 16) prouve que J_P a une suite de Jordan-Hölder dont les quotients sont formés de : λ_1 exemplaires de $\mathbb{Z}/p\mathbb{Z}$, et λ_2 exemplaires de μ_p. ■

3.3.2. Au facteur direct $\mathbb{H}_P$ de $\mathbb{H}_p$ correspond un idempotent ε_P. Rappelons que $T_p(J) = \varprojlim_m J_p m$ est le module de Tate de J en p ; notons-le T_p ; c'est un $\mathbb{H}_p$-module. Notons $T_P(J)$, ou T_P, le $\mathbb{H}_P$-module $\varepsilon_P . T_p(J)$.

La conjugaison complexe permet, puisque p est impair, de décomposer les espaces T_p, T_P et J_P, en somme directe de leurs sous-espaces propres correspondant aux valeurs propres $(+1)$ et (-1) : ainsi, $T_p = T_p^{(+)} \oplus T_p^{(-1)}$, $T_P = T_P^{(+1)} \oplus T_P^{(-1)}$, $J_P = J_P^{(+)} \oplus J_P^{(-)}$. L'accouplement de Weil définit une dualité entre $T_p^{(+)}$ et $T_p^{(-)}$, donc entre $T_P^{(+)} = \varepsilon_P . T_p^{(+)}$ et $T_P^{(+)} = \varepsilon_P . T_p^{(-)}$.

LEMME. (i) <u>Les $\mathbb{H}_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$-modules $T_p^{(+)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ et $T_p^{(-)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ sont libres de rang un</u> .

(ii) <u>Les $\mathbb{H}_P \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$-modules $T_P^{(+)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ et $T_P^{(-)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ sont libres de rang un</u> .

■ (i) L'algèbre $\mathbb{H} \otimes_{\mathbb{Z}} \mathbb{Q}$ se factorise en un produit de corps de nombres, donc $\mathbb{H}_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ est isomorphe à un produit de corps p-adiques : $\mathbb{H}_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq \prod_{i=1}^{k} L_i$. Cette $\mathbb{Q}_p$-algèbre opère sur $T_p^{(+)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, ce qui permet de décomposer $T_p^{(+)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ en somme directe de k espaces vectoriels sur $\mathbb{Q}_p$, le i-ème étant un espace vectoriel sur L_i, pour tout i de 1 à k. Et comme $\prod_{i=1}^{k} L_i$ opère fidèlement sur $T_p^{(+)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, le i-ème espace vectoriel est de dimension au moins égale à un sur L_i.

D'autre part, si l'un de ces espaces vectoriels était de dimension strictement supérieure à un sur le corps correspondant, alors la dimension de $T_p^{(+)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ sur $\mathbb{Q}_p$ serait strictement supérieure à celle de $\mathbb{H}_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Or ces deux dimensions sont égales à g : on a vu en (2.4.2) que $\mathbb{H}_p$ est un $\mathbb{Z}_p$-module libre de rang g, et en (II,5.1.1) que T_p est un $\mathbb{Z}_p$-module libre de rang $2g$; la dualité entre $T_p^{(+)}$ et $T_p^{(-)}$ montre que chacun est un $\mathbb{Z}_p$-module libre de rang g. Ceci prouve que $T_p^{(+)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ est libre de rang un sur $\mathbb{H}_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, et par dualité il en est de même pour $T_p^{(-)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

(ii) Comme $\mathbb{H}_P$ est facteur direct dans $\mathbb{H}_p$ (cf 2.4.2), la $\mathbb{Q}_p$-algèbre $\mathbb{H}_P \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ est aussi un produit de corps p-adiques, d'où la deuxième assertion du lemme. ∎

3.3.3. Rappelons que J_P (resp. C_p, Σ_p), est le groupe des points de J (resp. C, Σ) annulés par P (resp. p). Nous avons le résultat suivant :

PROPOSITION. Le $\mathbb{H}_P$-module $T_P(J)$ est libre de rang 2, et J_P est égal à $C_p \oplus \Sigma_p$.

∎ (i) Il est évident que $J_P^{(+)}$ contient C_p, et on peut montrer que $J_P^{(+)}$ est égal à C_p (cf. Mazur [21]).

(ii) D'autre part, on a : $T_P^{(-)}/P\,T_P^{(-)} \simeq T_p^{(-)}/P\,T_p^{(-)} \simeq J_p^{(-)}/P\,J_p^{(-)}$. Or l'accouplement de Weil, défini en (I.4.4) pour une courbe elliptique, se généralise à une variété abélienne quelconque. En particulier, il permet de définir une forme bilinéaire alternée non dégénérée de $J_p \times J_p$ dans μ_p, et alors $J_p^{(+)}$ et $J_p^{(-)}$ sont duaux l'un de l'autre. Donc le conoyau de P dans $J_p^{(-)}$ est isomorphe au noyau de P dans $J_p^{(+)}$, c'est-à-dire : $J_p^{(-)}/P \,.\, J_p^{(-)} \simeq J_P^{(+)}$. Donc $T_P^{(-)}/P.T_P^{(-)}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$; cela prouve que $T_P^{(-)}$ est un $\mathbb{H}_P$-module monogène ; on a : $T_P^{(-)} \simeq \mathbb{H}_P/\mathfrak{a}$ pour un

idéal $\mathfrak{A}$ de $\mathbb{H}_P$. On en déduit :

$$T_P^{(-)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq \mathbb{H}_P \otimes_{\mathbb{Z}_p} \mathbb{Q}_p / \mathfrak{A} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \ ;$$

or, on sait que $T_P^{(-)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ est un $\mathbb{H}_P \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$-module libre (cf 3.3.2), donc $\mathfrak{A} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ est nul. Mais $\mathbb{H}_P$ est libre sur $\mathbb{Z}_p$ (cf 2.4.2), donc $\mathfrak{A}$ est nul, et $T_P^{(-)} \simeq \mathbb{H}_P$.

(iii) Donc par dualité (cf 3.3.2), $T_P^{(+)}$ est lui aussi un $\mathbb{H}_P$-module libre de rang 1 , et la première assertion de la proposition est démontrée.

(iv) Enfin, $J_P^{(-)}$ contient Σ_p , et d'autre part on a, comme en (ii) , une suite d'isomorphismes :

$$J_P^{(-)} \simeq J_p^{(+)}/P.J_p^{(+)} \simeq T_p^{(+)}/P.T_p^{(+)} \simeq T_P^{(+)}/P.T_P^{(+)}$$
$$\simeq \mathbb{H}_P/P.\mathbb{H}_P \simeq \mathbb{Z}/p\mathbb{Z} \ .$$

(il s'agit d'isomorphismes de groupes, et pas de modules galoisiens). Donc $J_P^{(-)}$ est égal à Σ_p , et la proposition est "démontrée". ∎

3.3.4. *LEMME*. <u>La variété</u> $\mathcal{J} = J/\mathfrak{A}J$ <u>est un quotient de</u> $J^- = J(1+W)J$, <u>et</u> $\mathcal{J}_P$ <u>est isomorphe à</u> $C_p \oplus \Sigma_p$.

∎ Vérifions que $1+W$ appartient au noyau $\mathfrak{A}$ de l'application canonique (notée φ) de $\mathbb{H}$ dans $\mathbb{H}_P = \varprojlim_m \mathbb{H}/P^m$. Cela signifie que $\varphi(1+W)$ appartient à $\varphi(P^m)$ pour tout entier $m \geq 1$. Or $1+W$ est dans <u>Eis</u> (par définition), donc dans P ; pour $m > 1$, on remarque que $(1+W)^m = 2^{m-1}(1+W)$ (car $W^2 = 1$) , donc

$$\varphi(1+W) = \frac{1}{\varphi(2)^{m-1}} \varphi(1+W)^m$$

(car $\varphi(2)$ est inversible dans $\mathbb{H}_P$) ; ainsi, $\varphi(1+W)$ appartient à $\varphi(\underline{\text{Eis}}^m)$, donc à $\varphi(P^m)$, pour tout $m \geq 1$.

Enfin, $\mathcal{J}_P$ est isomorphe à J_P , c'est-à-dire à $C_p \oplus \Sigma_p$ (cf 3.3.3). ∎

4. *X(Q) EST FINI.*

Désormais, p désigne un facteur premier impair de n , et P l'idéal (Eis,p) de $\mathbb{H}$.

4.1. UN PEU DE COHOMOLOGIE... (cf Mazur [19a]).

4.1.1. Notons $\mathcal{G}$ le noyau et R l'image de l'application canonique de $\mathbb{H}$ dans $\mathbb{H}_P$ (donc $\mathcal{G} = \bigcap_{m\in\mathbb{N}} P^m$ et $R \simeq \mathbb{H}/\mathcal{G}$) . Notons $\mathcal{J}$ la variété abélienne $J/\mathcal{G}.J$, et $\mathcal{J}_S$ son schéma de Néron sur S (où S est l'anneau des entiers d'un corps de nombres K) . Le faisceau quotient $\mathcal{J}_S/\mathcal{J}_S^c$ est un schéma "en gratte-ciel" : il a un nombre fini de fibres non triviales, à savoir les fibres au-dessus des points $\wp$ divisant N , et chacune de ces fibres est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Notons $H^i(.)$ le i-ème groupe de cohomologie d'un faisceau en groupes (commutatifs) sur S pour la cohomologie fppf (cf EGA3 , SGA4...). En particulier, $H^0(.)$ est le groupe des "sections globales" au-dessus de S ; par exemple, $H^0(\mathcal{J}_S) \simeq \mathcal{J}(K)$, et $H^0(\mathcal{J}_S/\mathcal{J}_S^c) \simeq (\mathbb{Z}/p\mathbb{Z})^t$, si t désigne le nombre de places de K au-dessus de N . Notons A le groupe $H^0(\mathcal{J}_S) \simeq \mathcal{J}(K)$, et A^c le groupe $H^0(\mathcal{J}_S^c)$.

4.1.2. Nous allons maintenant évaluer la dimension (notée r_K) de A^c/PA^c sur $\mathbb{F}_p$. Si M est un faisceau en groupes sur Spec S annulé par p , notons $h^i(M)$ la dimension de $H^i(M)$ sur $\mathbb{F}_p$ (pour tout $i\in\mathbb{N}$)

LEMME . On a : $h^1(\mathcal{J}_{S,P}^c) = r_K + \dim_{\mathbb{F}_p}(H^1(\mathcal{J}_S^c)_P)$.

■ A la multiplication par p dans $\mathcal{J}_S^c$ est associée la suite exacte de schémas en groupes : $0 \to \mathcal{J}_{S,p}^c \to \mathcal{J}_S^c \xrightarrow{p} \mathcal{J}_S^c \to 0$. D'où la suite exacte longue de cohomologie :

$$0 \to H^0(\mathcal{J}^c_{S,p}) \to A^c \xrightarrow{p} A^c \to H^1(\mathcal{J}^c_{S,p}) \to H^1(\mathcal{J}^c_S) \xrightarrow{p} \dots ,$$

et donc la suite exacte courte :

$$0 \to A^c/pA^c \to H^1(\mathcal{J}^c_{S,p}) \to H^1(\mathcal{J}^c_S)_p \to 0 .$$

En fait, on peut considérer ceci comme une suite exacte de $R \otimes_{\mathbb{Z}} \mathbb{Z}_p$-modules, et alors les P-composantes forment une suite exacte de $\mathbb{F}_p$ espaces vectoriels :

$$0 \to A^c/P.A^c \to H^1(\mathcal{J}^c_{S,P}) \to H^1(\mathcal{J}^c_S)_P \to 0 ,$$

d'où le lemme. ∎

4.1.3. Notons r'_K la dimension de $H^1(\mathcal{J}^c_S)_P$ sur $\mathbb{F}_p$. Notons r (resp.2s) le nombre de places réelles (resp. complexes) du corps de nombres K ; t le nombre de places de K divisant N ; Pic(S) le groupe de Picard de S , (c'est-à-dire le groupe des classes d'idéaux de K) ; et $\rho_p(K)$ la dimension sur $\mathbb{F}_p$ de $\mathrm{Pic}(S)_p$, qui est égale à la dimension sur $\mathbb{F}_p$ de $\mathrm{Pic}(S)/p.\mathrm{Pic}(S)$.

THEOREME. Si K ne contient pas μ_p , alors on a :

$$r+s+t-2+\rho_p(K) \leq r_K+r'_K \leq r+s+t-2+2\rho_p(K) .$$

∎ (i) Nous allons utiliser les notations et résultats suivants : $(\mu_p)_S$ désigne le faisceau en groupes sur S de fibre constante μ_p ; si K ne contient pas μ_p , on a $H^0((\mu_p)_S) = 0$.

$(\mathbb{Z}/p\mathbb{Z})_S$ désigne le faisceau en groupes sur S de fibre constante $\mathbb{Z}/p\mathbb{Z}$; on a : $H^0((\mathbb{Z}/p\mathbb{Z})_S) \simeq \mathbb{Z}/p\mathbb{Z}$, et $H^1((\mathbb{Z}/p\mathbb{Z})_S)$ isomorphe au dual de $\mathrm{Pic}(S)/p\,\mathrm{Pic}(S)$.

$\widetilde{(\mathbb{Z}/p\mathbb{Z})}_S$ a pour fibre $\mathbb{Z}/p\mathbb{Z}$ en tout $\wp$ ne divisant pas N , et O en tout $\wp$ divisant N ; on a $H^0(\widetilde{(\mathbb{Z}/p\mathbb{Z})}_S) = 0$.

Φ_S est le faisceau quotient $(\mathbb{Z}/p\mathbb{Z})_S/\widetilde{(\mathbb{Z}/p\mathbb{Z})}_S$; sa fibre en $\wp$ est triviale, sauf si $\wp$ divise N , et dans ce cas c'est $\mathbb{Z}/p\mathbb{Z}$; on a $H^0(\Phi_S) \simeq (\mathbb{Z}/p\mathbb{Z})^t$ et $H^1(\Phi_S) = 0$.

$(G_m)_S$ est le faisceau en groupes sur S défini par le groupe multiplicatif ; on a : $H^0(G_m) \simeq S^*$, $H^1(G_m) \simeq \mathrm{Pic}(S)$, et $H^2(G_m)_p = 0$.

(ii) Nous allons maintenant évaluer $h^1(\mathcal{J}^c_{S,P})$; la suite exacte de faisceaux en groupes :

$$0 \to (\mu_p)_S \to \mathcal{J}^c_{S,P} \to (\widetilde{\mathbb{Z}/p\mathbb{Z}})_S \to 0$$

(qui vient de $\mathcal{J}_P \simeq \mu_p \oplus \mathbb{Z}/p\mathbb{Z}$ (3.3.4) et de la description de $\mathcal{J}_S/\mathcal{J}^c_S$ (4.1.1)), donne en cohomologie la suite exacte longue :

$$0 \to 0 \to H^0(\mathcal{J}^c_{S,P}) \to 0 \to H^1((\mu_p)_S) \to H^1(\mathcal{J}^c_{S,P}) \to H^1((\widetilde{\mathbb{Z}/p\mathbb{Z}})_S) \to H^2((\mu_p)_S) \to \cdots .$$

D'où la double inégalité :

$$(*) \quad h^1((\mu_p)_S) + h^1((\widetilde{\mathbb{Z}/p\mathbb{Z}})_S) \geq h^1(\mathcal{J}^c_{S,P}) \geq h^1((\mu_p)_S) + h^1((\widetilde{\mathbb{Z}/p\mathbb{Z}})_S) - h^2((\mu_p)_S) .$$

D'autre part, la suite exacte de Kummer :

$$0 \to (\mu_p)_S \to (G_m)_S \xrightarrow{p} (G_m)_S \to 0$$

donne en cohomologie la suite exacte :

$$0 \to 0 \to S^* \xrightarrow{p} S^* \to H^1((\mu_p)_S) \to \mathrm{Pic}(S) \xrightarrow{p} \cdots$$

d'où la suite exacte :

$$0 \to S^*/pS^* \to H^1((\mu_p)_S) \to \mathrm{Pic}(S)_p \to 0 .$$

Or, d'après le théorème de Dirichlet (cf [33] ,4.4) , S^* est isomorphe à $\mathbb{Z}^{r+s-1} \times G$, où G est le groupe des racines de l'unité contenues dans K . Comme K ne contient pas μ_p , S^*/S^{*p} est isomorphe à $\mathbb{F}_p^{r+s-1}$; d'où :

$$h^1((\mu_p)_S) = r + s - 1 + \rho_p(K) .$$

La même suite exacte de Kummer donne aussi, en cohomologie, la suite exacte :

$$0 \to \mathrm{Pic}(S)/p.\mathrm{Pic}(S) \to H^2((\mu_p)_S) \to 0 ,$$

d'où $h^2((\mu_p)_S) = \rho_p(K)$.

Enfin, la suite exacte : $0 \to (\widetilde{\mathbb{Z}/p\mathbb{Z}})_S \to (\mathbb{Z}/p\mathbb{Z})_S \to \Phi_S \to 0$ donne en cohomologie la suite exacte :

$$0 \to \mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^t \to H^1((\mathbb{Z}/p\mathbb{Z})_S) \to H^1(\mathbb{Z}/p\mathbb{Z})_S) \to 0$$

où $h^1((\mathbb{Z}/p\mathbb{Z})_S) = \rho_p(K)$, d'où $h^1((\widetilde{\mathbb{Z}/p\mathbb{Z}})_S) = t - 1 + \rho_p(K)$. En reportant ces résultats dans la double inégalité (*) , et en utilisant le lemme (4.1.2) on obtient le théorème. ∎

4.1.4. Rappelons que r_K désigne la dimension de $A^C/P.A^C$ sur $\mathbb{F}_p$. Le théorème (4.1.3) nous permettra de montrer que, sous certaines hypothèses, r_K est nul. Nous utiliserons ensuite le résultat suivant :

LEMME. Si r_K est nul, alors le groupe A est de torsion.

∎ Si r_K est nul, les $\mathbb{H}$-modules A^C et $P.A^C$ sont égaux. Or A^C peut être considéré comme un R-module, donc (en notant P_R l'image de P dans R), les R-modules A^C et $P_R.A^C$ sont égaux. Notons $R_p = R \otimes_{\mathbb{Z}} \mathbb{Z}_p$, $A_p^C = A^C \otimes_{\mathbb{Z}} \mathbb{Z}_p$, et $P_{R_p} = P_R \otimes_{\mathbb{Z}} \mathbb{Z}_p$; alors les R_p-modules A_p^C et $P_{R_p}.A_p^C$ sont égaux.

Nous allons montrer que R_p est un anneau local ; alors P_{R_p} est son seul idéal maximal, et le lemme de Nakayama ([1a] ,2.6) prouve que A_p^C est nul, donc que A^C est un groupe de torsion. Comme A et A^C ne diffèrent que par un groupe fini (cf. 4.1.1), on en déduit que A est un groupe de torsion.

Enfin, montrons que R_p est un anneau local : considérons l'anneau local $R_P = \varprojlim_m R/P_R^m = \varprojlim_m \mathbb{H}/P^m$. C'est un facteur local de R_p (ceci est analogue à l'étude de $\mathbb{H}$, $\mathbb{H}_p$, $\mathbb{H}_P$ faite en 2.4.2). Or le noyau de la projection canonique de R_p sur R_P est égal à l'intersection des P_R^m , et comme R est justement égal à $\mathbb{H}/\bigcap_m P^m$, ce noyau est nul, et $R_p = R_P$ est un anneau local. ∎

4.2. APPLICATION : FINITUDE DE $X(\mathbb{Q})$.

4.2.1. Rappelons que N est un nombre premier, supérieur ou égal à 11 et différent de 13 .

THEOREME. (Mazur, [21]) Il existe un quotient $\mathcal{J}$ non trivial de J , tel que $\mathcal{J}(\mathbb{Q})$ soit fini.

■ Nous pouvons maintenant démontrer ce théorème si n n'est pas une puissance de 2 (c'est-à-dire si N n'est pas de la forme $1+2^{\lambda}$ ou $1+3.2^{\lambda}$, $\lambda \in \mathbb{N}$) ; lorsque n est une puissance de 2 , voir [21] .

Soit p un nombre premier impair divisant n ; appliquons le théorème (4.1.3) à $K = \mathbb{Q}$. Alors $r = 1$, $s = 0$, $t = 1$, $\rho_p(\mathbb{Q}) = 0$, et l'on obtient : $r_K + r'_K = 0$, c'est-à-dire : $r_K = r'_K = 0$. Le lemme (4.1.4) prouve alors que $A = \mathcal{J}(\mathbb{Q})$ est fini. D'autre part, $\mathcal{J}$ est non trivial, puisque $\mathcal{J}_p$ est d'ordre p^2 (cf 3 .3.4). ■

4.2.2. *COROLLAIRE* . Si N est un nombre premier, $N \geq 11$, et $N \neq 13$ alors $X_o(N)(\mathbb{Q})$ est fini. (cf [21] et [22] , théorème 3).

■ Notons $\mathcal{X}$ l'image de X dans $\mathcal{J}$ par l'application canonique : $X \to J \to \mathcal{J}$; comme X engendre J , $\mathcal{X}$ engendre $\mathcal{J}$; et comme $\mathcal{J}$ est non trivial, $\mathcal{X}$ est une courbe, et les fibres de : $X \to \mathcal{X}$ sont finies. Puisque $\mathcal{J}(\mathbb{Q})$ est fini (4.2.1), $\mathcal{X}(\mathbb{Q})$ l'est aussi, et $X(\mathbb{Q})$ est fini. ■

4.2.3. Supposons maintenant que K est un corps quadratique imaginaire : $K = \mathbb{Q}(\sqrt{-d})$, où d est un entier positif sans facteur carré. Supposons de plus que K est différent de $\mathbb{Q}(\sqrt{-3})$ si $p = 3$; alors K ne contient pas μ_p . Dans ce cas, $r = 0$, $s = 1$ et $t = 1$ si N est ramifié ou inerte dans $K/\mathbb{Q}$, $t = 2$ si N est décomposé ; c'est-à-dire : $t = 1$ si $(\frac{-d}{N}) = 0$ ou -1 , et $t = 2$ si $(\frac{-d}{N}) = 1$ (cf [33] ,5.4) . Le théorème (4.1.3) devient donc ici :

$$\text{si } \left(\frac{-d}{N}\right) = 0 \text{ ou } -1 \text{ , } \quad \rho_p(K) \leq r_K + r'_K \leq 2\rho_p(K)$$

$$\text{si } \left(\frac{-d}{N}\right) = 1 \quad \text{ , } \quad 1+\rho_p(K) \leq r_K + r'_K \leq 2\rho_p(K) \text{ .}$$

PROPOSITION . Si N n'est pas décomposé dans $K/\mathbb{Q}$, et s'il existe un nombre premier impair p tel que p divise n et p ne divise pas le nombre de classes de K , alors $\mathcal{J}(K)$ et $X(K)$ sont finis.

■ En effet, dans ce cas, $t = 1$ et $\rho_p(K) = 0$, donc $r_K = r'_K = 0$, et le $\mathbb{Z}$-rang de $\mathcal{J}(K)$ est fini. ■

4.2.4. Remarque : On peut associer à J un groupe sur lequel $\mathbb{H}$ opère, appelé groupe de Tate-Šafarevič et noté Ш (cf [5] ,[20]). On peut montrer que les p-composantes de $Ш(K)$ et de $H^1(\mathcal{J}_S^c)$ coïncident pour tout p impair ([20] , appendice). Donc r'_K est la dimension de $Ш(K)_P$ sur $\mathbb{F}_p$, et le théorème (4.1.3) permet de limiter à la fois la valeur de r_K (c'est ce que nous utilisons) et celle de $\dim_{\mathbb{F}_p}(Ш(K)_P)$.

En particulier, nous venons de montrer que le groupe des points de Ш annulés par P et rationnels sur K est réduit à 0 dans les cas suivants : lorsque $K = \mathbb{Q}$ (4.2.1), et lorsque K est un corps quadratique imaginaire vérifiant les hypothèses de la proposition (4.2.3).

4.3. QUELQUES APPLICATIONS ARITHMETIQUES.

Nous démontrons ici, à partir du théorème (4.1.3), des propriétés de divisibilité de certains corps quadratiques. Plus précisément, nous appliquons le théorème (4.1.3) lorsque $N = 11$ (resp. $N = 23$), cette valeur correspondant à une courbe modulaire $X_o(N)$ elliptique (resp. hyperelliptique).

Remarque : nous avons montré (en 3.2.4) que $J(\mathbb{Q})$ est égal à C . Nous allons le redémontrer directement lorsque $N = 11$ ou 23 .

4.3.1. Le cas $N = 11$.

Dans ce cas, $n = 5$ est un nombre premier impair, et le genre de X est égal à 1, donc X coïncide avec sa jacobienne J ; nous avons étudié la courbe elliptique X en (II.8) : elle a une équation de la forme : $y^2+y = x^3 - x^2 - 10x - 20$, ou encore : $(y+\frac{1}{2})^2 = x^3 - x^2 - 10x - 20 + \frac{1}{4}$.

Pour tout rationnel x , notons $d(x)$, ou d , le rationnel $x^3 - x^2 - 10x - 20 + \frac{1}{4}$.

PROPOSITION. Soit K un corps quadratique ; alors les groupes de torsion de $X(K)$ et $X(\mathbb{Q})$ sont tous les deux égaux à C .

■ Comme C est isomorphe à $\mathbb{Z}/5\mathbb{Z}$, et comme on a les inclusions : $C \subset X(\mathbb{Q}) \subset X(K)$, il suffit de vérifier que le groupe de torsion de $X(K)$ est d'ordre 5 . Comme $X_0(11)$ a bonne réduction modulo 2 , la ℓ-composante du groupe de torsion de $X(K)$, pour nombre premier impair ℓ, s'envoie injectivement dans $\widetilde{X}(\widetilde{K})$ (si le tilde indique la réduction modulo 2) (cf II,6.2.2) ; comme $\widetilde{K}$ est égal à $\mathbb{F}_2$ ou $\mathbb{F}_4$, l'ordre de $\widetilde{X}(\widetilde{K})$ est au plus égal à 9 . Mais d'autre part, c'est un multiple de 5 , donc l'ordre de $\widetilde{X}(\widetilde{K})$ est égal à 5 . Il suffit maintenant de vérifier que $X(K)$ n'a aucun point d'ordre 2 . Or les points d'ordre 2 de X sont les points de coordonnées $(\alpha, -\frac{1}{2})$, où α est une racine du polynôme $x^3-x^2-10x-20+\frac{1}{4}$. Comme ces points ne sont pas rationnels sur $\mathbb{Q}$, le degré de l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est égal à 3 , et α ne peut pas être dans K . Ainsi, le groupe de torsion de $X(K)$ est d'ordre 5 . ■

COROLLAIRE. Si d est strictement négatif, et si 11 n'est pas décomposé dans l'extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, alors le nombre de classes de K est divisible par 5 .

■ Le corps $K = \mathbb{Q}(\sqrt{d})$ est construit de sorte que $X_0(11)$ contienne un point rationnel sur K et non sur $\mathbb{Q}$, à savoir le point $P_0 = (x, \sqrt{d} - \frac{1}{2})$. D'après la proposition qui précède, P_0 n'est pas un point de torsion de $X(K)$, donc le $\mathbb{Z}$-rang de $J(K)$ est strictement positif.

Mais ici, J est égal à $\mathcal{J}$: en effet, $\mathbb{H}_p$ est libre de rang 1 sur $\mathbb{Z}_p$ (cf 2.4.2) , donc $\mathbb{H}_p$ est égal à $\mathbb{H}_P$, et l'homomorphisme canonique de $\mathbb{H}$ dans $\mathbb{H}_P$ est injectif ; ainsi, $\mathfrak{a}$ est nul, et J égal à $\mathcal{J} = J/\mathfrak{a}J$.

Mais alors, le théorème (4.1.3), où $r = 0$, $s = 1$, $t = 1$, $p = n = 5$, prouve que $\rho_5(K)$ est strictement positif, c'est-à-dire que 5 divise l'ordre du groupe de Picard de S , qui est égal au nombre de classes de K . ∎

Voici un tableau donnant, pour quelques valeurs de x , les valeurs correspondantes de : $4d = 4x^3 - 4x^2 - 40x - 79$, $(\frac{4d}{11})$, et $h(\mathbb{Q}(\sqrt{d}))$; on vérifie que $h(\mathbb{Q}(\sqrt{d}))$ est divisible par 5 lorsque $(\frac{4d}{11})$ est égal à 0 ou -1 .

x	4d	$(\frac{4d}{11})$	$h(\mathbb{Q}(\sqrt{d}))$
4	-47	-1	5
3	-127	+1	5
2	-143	0	10
1	-119	-1	10
0	-79	+1	5
-1	-47	-1	5
-2	-47	-1	5
-3	-103	-1	5
-4	-239	+1	15
-5	-479	+1	25
-6	$-847 = -7\times11^2$	+1	1
-7	-1367	-1	25
-8	-2063	+1	45
-9	-2959	0	40
-10	-4079	-1	85
-11	-5447	+1	60
-12	-7087	-1	30
-13	-9023	-1	80

4.3.2. Le cas $N = 23$.

Dans ce cas, $n = 11$ est un nombre premier impair, le genre g de X est égal à 2 , et le genre g_+ de X_+ est nul (cf 1.2) ; X est une courbe hyperelliptique. Tous les points rationnels sur la jacobienne J de X sont de torsion : en effet, d'une part la dimension de J_+ est égale à celle de $J(X_+)$ (d'après 1.1.2), donc à g_+ , qui est nul ; et d'autre part, on montre (cf[22]) que J^- (c'est-à-dire J/J_+) est égal à $\mathcal{J}$; or le $\mathbb{Z}$-rang de $\mathcal{J}(\mathbb{Q})$ est nul d'après (4.2.1).

PROPOSITION. Soit K un corps quadratique ; alors les groupes de torsion de $J(K)$ et $J(\mathbb{Q})$ sont tous les deux égaux à C .

▪ Soient ℓ un nombre premier différent de N , et m un entier strictement positif. Notons $\widetilde{X}$ (resp. $\widetilde{J}$) la réduction de X (resp. de J) modulo ℓ , et rappelons comment on peut calculer les cardinaux de $\widetilde{X}(\mathbb{F}_{\ell^m})$ et de $\widetilde{J}(\mathbb{F}_{\ell^m})$: si α_1 , α_2 , ... , α_{2g} désignent les valeurs propres de l'endomorphisme de Frobenius π_ℓ sur le module de Tate $T_\ell(J)$, ordonnées de sorte que $\alpha_{g+i} = \bar{\alpha}_i$ $(1 \le i \le g)$ (rappelons que $\alpha_i \cdot \bar{\alpha}_i = \ell$, cf II,7.3.2) , et si $a_\ell^{(i)}$ désigne la trace $\alpha_i + \bar{\alpha}_i$ $(1 \le i \le g)$, alors on a les formules suivantes :

$$\#\widetilde{X}(\mathbb{F}_{\ell^m}) = 1 + \ell^m - \sum_{i=1}^{2g} \alpha_i^m \ ,$$

et en particulier

$$\#\widetilde{X}(\mathbb{F}_\ell) = 1 + \ell - \sum_{i=1}^{g} a_\ell^{(i)} \quad \text{(cf II,7.3.2)} \ ;$$

et

$$\#\widetilde{J}(\mathbb{F}_{\ell^m}) = \prod_{i=1}^{2g} (1-\alpha_i^m) = \prod_{\zeta \in \mu_m} \prod_{i=1}^{g} (\zeta-\alpha_i)(\zeta-\bar{\alpha}_i) = \prod_{\zeta \in \mu_m} \prod_{i=1}^{g} (\zeta^2 - \zeta a_\ell^{(i)} + \ell)$$

(cf [23a] ,21,thm.4).

Nous allons appliquer ces formules lorsque $\ell = 2$ ou 3 ; pour cela, calculons les valeurs des $a_\ell^{(i)}$; rappelons que les nombres $a_\ell^{(i)}$ $(1 \le i \le g)$ sont les valeurs propres de l'opérateur de Hecke T_ℓ , considéré comme endomorphisme de J (cf II,7.4.3).

LEMME (cf [51]). Les opérateurs de Hecke T_2 et T_3 vérifient : $T_2^2 + T_2 - 1 = 0$, et $T_3^2 = 5$; l'algèbre de Hecke $\mathbb{H}$ est isomorphe à l'anneau de Dedekind $\mathbb{Z}[\frac{-1+\sqrt{5}}{2}]$.

Admettons provisoirement ce lemme, et terminons la démonstration de la proposition : nous obtenons pour $a_2^{(i)}$ $(i=1,2)$ les zéros de X^2+X-1, à savoir $\frac{-1\pm\sqrt{5}}{2}$, et pour $a_3^{(i)}$ $(i=1,2)$ les zéros de X^3-5, à savoir $\pm\sqrt{5}$. D'où :

$$\#\tilde{X}(\mathbb{F}_2) = \#\tilde{X}(\mathbb{F}_3) = 4 ;$$

$$\#\tilde{J}(\mathbb{F}_2) = \#\tilde{J}(\mathbb{F}_3) = 11 ;$$

$$\#\tilde{J}(\mathbb{F}_4) = 11\times 5 ; \quad \#\tilde{J}(\mathbb{F}_9) = 11^2 .$$

Or, la proposition (II,6.2.2) se généralise aux variétés abéliennes de genre quelconque : si une variété abélienne V définie sur un corps de nombres L a bonne réduction modulo un idéal premier $\mathfrak{P}$, et si ℓ désigne le nombre premier que divise $\mathfrak{P}$, alors la réduction modulo $\mathfrak{P}$, restreinte à la composante ℓ-primaire du groupe de torsion de $V(L)$, est injective.

En appliquant ceci à $\ell = 2$ et 3, et aux corps de nombres $\mathbb{Q}$ et K, les calculs précédents montrent que les groupes de torsion de $J(\mathbb{Q})$ et de $J(K)$ sont tous les deux d'ordre 11. ∎

Démontrons maintenant le lemme :

∎ Si $N \equiv -1 \pmod{12}$, nous avons vu (cf 2.1.3) que la fonction $f = \eta^2\eta_N^2$ est une forme parabolique de poids 2 pour $\Gamma_0(N)$. De plus,

$$f|_2 W = f|_2 \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} = N(N\tau)^{-2}\cdot\eta^2\left(\frac{-1}{N\tau}\right)\cdot\eta^2\left(\frac{-1}{\tau}\right) ;$$

comme $\eta(\frac{-1}{\tau}) = \sqrt{\frac{\tau}{i}}\cdot\eta(\tau)$ (cf I,2.3.4), on a $f|_2 W = -f$.

En particulier, lorsque $N = 23$, $f(\tau) = q^2\prod_{n=1}^{\infty}(1-q^n)^2\prod_{n=1}^{\infty}(1-q^{23n})^2$; comme son développement de Fourier n'a pas de terme de degré 1 en q, ce n'est pas une fonction propre des opérateurs de Hecke, donc f et $f|_2 T_2$ sont linéairement indépendantes. D'autre part, le genre g de

$X_0(23)$ est égal à 2 , donc la dimension de l'espace $S(2,23)$ des formes paraboliques de poids 2 pour $\Gamma_0(23)$ est égal à 2 (cf II,4.1.5), et $\{f, f|_2 T_2\}$ en forme une base. Il y a donc une relation de dépendance linéaire entre f , $f|_2 T_2$, et $f|_2 T_2^2$. Si une forme parabolique g a pour développement de Fourier $\sum_{m=1}^{\infty} a_m q^m$, alors $g|_2 T_2$ a pour développement de Fourier $\sum_{m=1}^{\infty} (2a_{m/2} + a_{2m}) q^m$. Ici,

$$f(\tau) \equiv q^2 - 2q^3 - q^4 + 2q^5 + q^6 + 2q^7 - 2q^8 \pmod{q^9} ,$$

donc

$$f|_2 T_2(\tau) \equiv q - q^2 + q^3 \pmod{q^5} ,$$

et

$$f|_2 T_2^2(\tau) \equiv -q + 2q^2 \pmod{q^3} ,$$

d'où

$$f|_2 (T_2^2 + T_2 - 1) \equiv 0 \pmod{q^3} .$$

Montrons qu'en fait, $f|_2 (T_2^2 + T_2 - 1)$ est nulle ; soit ω la forme différentielle holomorphe $f|_2 (T_2^2 + T_2 - 1)(\tau) d\tau$; comme $d\tau = \frac{1}{2\pi i} \frac{\omega q}{q}$, ω possède, à l'infini, un zéro d'ordre supérieur ou égal à $3-1 = 2$, et la forme différentielle holomorphe $\omega \circ W$ a un zéro d'ordre ≥ 2 à la pointe 0 . Or $\omega + \omega \circ W$ est une forme différentielle holomorphe sur X_+ , dont le genre g_+ est nul : cette forme différentielle est donc nulle, et $\omega = -\omega \circ W$ a un zéro d'ordre ≥ 2 à chaque pointe, donc le degré de ω est ≥ 4 . Par ailleurs, si $\omega \neq 0$, $\deg(\omega) = 2g - 2 = 2$. Ainsi ω est nulle et $f|_2 (T_2^2 + T_2 - 1) = 0$. On en déduit que $(f|_2 T_2)|_2 (T_2^2 + T_2 - 1) = 0$, puisque T_2 commute à $T_2^2 + T_2 - 1$, donc que $T_2^2 + T_2 - 1$ annule tout l'espace $S(2,23)$.

Ainsi, dans l'algèbre de Hecke $\mathbb{H}$, T_2 est racine de l'équation du second degré : $X^2 + X - 1 = 0$, autrement dit $T_2 = \frac{-1 \pm \sqrt{5}}{2}$; or l'anneau $\mathbb{Z}[\frac{-1+\sqrt{5}}{2}]$ est l'ordre maximal de $\mathbb{Q}(\sqrt{5})$; comme $\mathbb{H}$ est un $\mathbb{Z}$-module libre de rang $g = 2$ (cf 2.4.2) contenant $\mathbb{Z}[T_2]$, on a exactement : $\mathbb{H} = \mathbb{Z}[T_2]$, et cet anneau est de Dedekind.

Enfin, un calcul analogue à celui affectué pour T_2 prouve que T_3 est racine de l'équation : $T_3^2 = 5$. ∎

COROLLAIRE . Soient x un rationnel, $d = (x^3-x+1)(x^3-8x^2+3x-7)$, et $K = \mathbb{Q}(\sqrt{d})$. Supposons que d est strictement négatif, et que 23 ne se décompose pas dans l'extension $K/\mathbb{Q}$. Alors le nombre de classes $h(K)$ de K est divisible par 11 .

Ce résultat est analogue au corollaire de la proposition (4.3.1), mais la démonstration est un peu différente car ici X n'est pas une courbe elliptique ; nous utilisons des résultats qui seront démontrés dans le paragraphe 5 .

■ Remarquons d'abord que l'équation :

$$y^2 = (x^3 - x + 1)(x^3 - 8x^2 + 3x - 7)$$

est une équation de X (cf [9]) .

Il existe donc un point P de X rationnel sur K mais pas sur $\mathbb{Q}$. On lui fait correspondre l'image du diviseur $(P) - (WP)$ dans $J^-(K)$ qui coïncide ici avec $\mathcal{J}(K)$. Si 11 ne divise pas $h(K)$, alors $\rho_{11}(K) = 0$ et le théorème (4.1.3) prouve que ce point de $\mathcal{J}(K)$ est un point de torsion; mais alors, il est rationnel sur $\mathbb{Q}$, d'après la proposition qui précède. Notons σ le générateur de $\mathrm{Gal}(K/\mathbb{Q})$: donc $(\sigma P) - (\sigma WP)$ et $(P) - (WP)$ ont la même image dans J ; or nous verrons en (5.2.3) que ceci prouve que P est égal à σP ou à WP . Comme P n'est pas rationnel sur $\mathbb{Q}$, il est différent de σP ; et d'autre part, nous verrons en (5.2.4, remarque) que W n'a pas de point fixe rationnel sur K car le nombre de classes de $\mathbb{Q}(\sqrt{-23})$ est égal à 3 . Ainsi, l'hypothèse faite sur $h(K)$ nous mène à une contradiction ; donc 11 divise $h(K)$. ■

Exemple : pour $x = \frac{3}{2}$, le corps K est égal à $\mathbb{Q}(\sqrt{-3151})$ et son nombre de classes est égal à 22 .

5. *APPENDICES.*

Nous supposons toujours N premier, $N \geq 11$ et $N \neq 13$, donc $X_0(N)$ de genre $g \geq 1$.

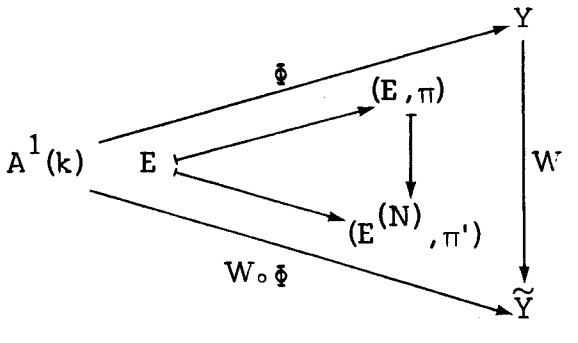
5.1. FIBRE EN N DU SCHEMA DE NERON DE J .

Notre but est d'indiquer ici comment on peut démontrer une partie du théorème admis en (3.1.2) : $J_{/N} \simeq \overline{C} \times J^{c}_{/N}$.

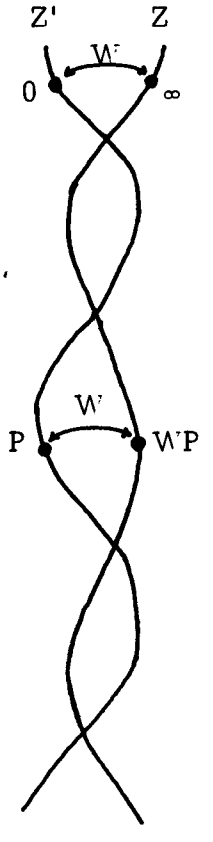
5.1.1. Notons maintenant $\widetilde{X}$ la réduction modulo N de $X_0(N)(K)$, où K est corps de nombres, et k le corps résiduel de K (mod.N) : k est une extension finie de $\mathbb{F}_N$, donc un corps parfait de caractéristique N , et $\widetilde{X}$ est défini sur k . Notons $\widetilde{J}$ la jacobienne de $\widetilde{X}$.

En caractéristique N , on interprète $\widetilde{X}$ comme la réunion des deux pointes ∞ et 0 , et la courbe $\widetilde{Y}$, formée des couples (E,λ) où E est une courbe elliptique, λ une isogénie de degré N de E dans une courbe elliptique E' , le couple (E,λ) étant défini sur k . Or, on a vu (cf II,5.5) que les seules isogénies de degré N d'une courbe elliptique E en caractéristique N sont : l'endomorphisme de Frobenius $\pi = \pi_N$ de E dans $\pi(E)$ (noté $E^{(N)}$) , et l'endomorphisme transposé $\pi' = \pi'_N$ de $E^{(N)}$ dans E . Le premier est toujours inséparable, le second l'est si et seulement si E est supersingulière.

Notons Φ l'application de $A^1(k)$ dans $\widetilde{X}$ qui associe, à la classe de courbes elliptiques E d'invariant j , la classe des couples (E,π) dans $\widetilde{Y}$. On remarque que $W((E,\pi)) = (E^{(N)},\pi')$ (cf II,5.2.4), ce qui donne le diagramme commutatif :



On peut donc considérer $\widetilde{X}$ comme formé de 2 exemplaires Z et Z' de la droite projective $\mathbb{P}^1(k)$, Z étant formé des classes des couples (E,π) , et Z' des classes des couples $(E^{(N)},\pi')$ ces couples se correspondant par l'involution d'Atkin-Lehner W . Les points d'intersection de Z et



Z' correspondent aux courbes supersingulières pour lesquelles (E,π) et $(E^{(N)},\pi')$ sont isomorphes ; ils sont en nombre fini (cf II,5.5.2).
Les pointes 0 et ∞ de $\widetilde{X}$ sont échangées par l'action de W. Nous avons vu que, sur X, la pointe ∞ peut être regardée comme la "limite" des couples $(\mathbb{C}^*/q^{\mathbb{Z}},\mu_N)$ lorsque q tend vers 0 ; comme μ_N est le noyau de π dans $\mathbb{C}^*/q^{\mathbb{Z}}$, la pointe ∞ de $\widetilde{X}$ est sur Z ; et alors la pointe 0 est sur Z'. Elles sont toujours distinctes.

5.1.2. Genre arithmétique et produit d'intersection.

Il s'agit ici de "décrire" ces notions et d'indiquer, parmi leurs propriétés, celles que nous utiliserons. On trouve dans [42] ou [35], par exemple, des définitions et démonstrations précises.

Considérons une surface fibrée Σ au-dessus de Spec $\mathbb{Z}$, et notons $\mathcal{C}$ le groupe des diviseurs sur Σ, c'est-à-dire le groupe abélien libre engendré par les courbes tracées sur Σ. On définit une application bilinéaire symétrique de $\mathcal{C}\times\mathcal{C}$ dans $\mathbb{N}\cup\{+\infty\}$, appelée produit d'intersection, et noté $(-\cdot-)$, de la manière suivante : si D et D' sont deux courbes sur $\mathcal{C}$, leur produit d'intersection $(D.D')$ est égal au nombre de leurs points d'intersection, en tenant compte de leur "multiplicité" ; cette définition est étendue par bilinéarité à $\mathcal{C}\times\mathcal{C}$.

D'autre part, étant donné une courbe D, en plus du genre (dit "géométrique") de la normalisée $\overline{D}$ de D, noté $g(\overline{D})$, on définit le

genre arithmétique de D , noté $p_a(D)$ (cf [8] , [35]). Lorsque les seules singularités de D sont des points doubles à tangentes distinctes (en nombre égal à s), ces deux notions sont liées par : $p_a(D) = g(\overline{D}) + s$. La formule de "Riemann-Roch pour les surfaces" permet de prolonger p_a à tous les diviseurs : $p_a(D+D') = p_a(D) + p_a(D') - 1 - (D \cdot D')$ (cf [35]).

Le genre arithmétique est invariant par éclatement, ce qui permet de se ramener au cas où tous les points multiples sont des points doubles à tangentes distinctes.

Il est aussi invariant par spécialisation, donc on peut le calculer en caractéristique nulle, ou en réduction modulo p pour n'importe quel nombre premier p .

5.1.3. *LEMME* . Le nombre de points supersinguliers sur $\widetilde{X}$ est égal à $g+1$; ils sont tous définis sur $\mathbb{F}_{N^2}$, et le nombre de points supersinguliers de $\widetilde{X}$ qui ne sont pas définis sur $\mathbb{F}_N$ est égal à $2g_+$.

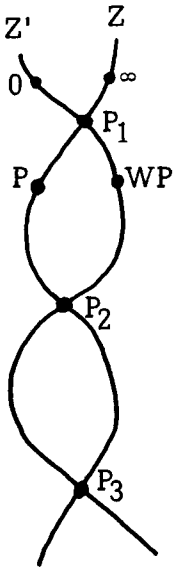
■ Calculons le genre arithmétique de X :

D'une part, en caractéristique nulle, il n'y a pas de point double donc $p_a(X) = g$; d'autre part, $p_a(X)$ est égal à $p_a(\widetilde{X})$, c'est-à-dire à $-1 + p_a(Z) + p_a(Z') + (Z.Z')$. Or $p_a(Z) = p_a(Z) = 0$ (car Z et Z' sont de genre -géométrique- nul), et $(Z \cdot Z')$ est le nombre de points d'intersection de Z et Z' , c'est-à-dire le nombre de points supersinguliers sur $\widetilde{X}$. (en effet, ce sont tous des points d'intersection simple). D'où la première assertion.

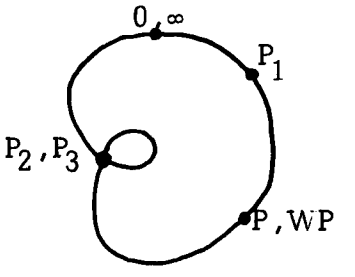
De manière analogue, calculons le genre arithmétique de $X_+ = X/W$; il n'y a pas de point double sur X_+ , donc $p_a(X_+) = g_+ = p_a(X/W)$; rappelons que W échange Z et Z' . Nous venons de voir que tous les points supersinguliers sont définis sur $\mathbb{F}_{N^2}$. Notons r (resp. $2s$) le nombre de ceux qui sont définis sur $\mathbb{F}_N$ (resp. sur $\mathbb{F}_{N^2} \setminus \mathbb{F}_N$) . Faire le quotient de $\widetilde{X}$ par W , sur $\mathbb{F}_N$, revient à identifier Z et Z' , et à identifier les points supersinguliers conjugués sur $\mathbb{F}_N$. On obtient ainsi une courbe

de genre géométrique nul, avec s points doubles à tangentes distinctes. D'où $p_a(\tilde{X}/W) = s$.

$\tilde{X}$:



$\tilde{X}/W$:



(ici P_1 est défini sur $\mathbb{F}_N$, P_2 et P_3 sont conjugués sur $\mathbb{F}_N$; $r = s = 1$).

5.1.4. Les points d'intersection de Z et Z' sont tous simples, mais les tangentes ne sont distinctes que si ces points correspondent à un invariant j différent de 0 et 12^3 . Si un point d'invariant $j = 0$ (resp. $j = 12^3$) est supersingulier, il faut l'éclater en 2 droites (resp. 1 droite) pour se ramener à des points d'intersection simples à tangentes distinctes (cf [1] , II, De-Ra, 6,16) .

Nous allons voir d'abord pour quelles valeurs de N ces points sont supersinguliers ; ensuite nous étudierons la courbe obtenue par éclatement de $\tilde{X}$.

PROPOSITION. Soit E une courbe elliptique d'invariant j sur un corps fini k de caractéristique $N \geq 5$. Si $j = 0$ (resp. $j = 12^3$) , la courbe E est supersingulière si et seulement si $N \equiv -1$ (mod.6) (resp. $N \equiv -1$ (mod.4)) .

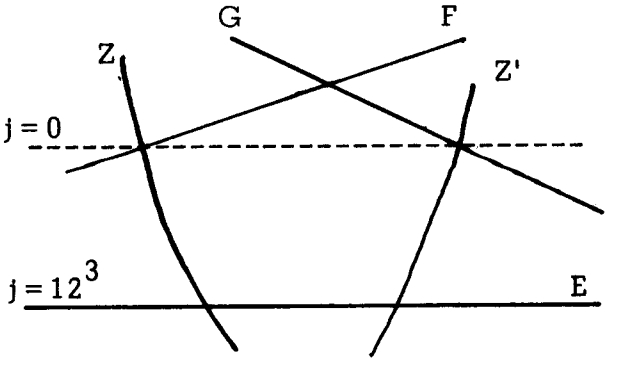
Remarque : N est impair, donc on a toujours $N \equiv -1$ (mod.2) .

■ Supposons que $j = 12^3$. Alors le groupe des automorphismes

de E (sur $\bar{k}$) est cyclique d'ordre 4 , donc l'anneau End E des endomorphismes de E (sur $\bar{k}$) contient $\mathbb{Z}[i]$. Si $N \equiv -1 \pmod 4$, N n'est pas décomposé dans $\mathbb{Z}[i]$; or $N = \pi_N \cdot \pi'_N$, d'où $\mathbb{Z}[\pi_N] \not\subset \mathbb{Z}[i]$; donc End E , qui contient $\mathbb{Z}[\pi_N, i]$, n'est pas un ordre dans un corps quadratique. D'après un théorème de Deuring (cf II,5.5.3), cela prouve que End $E \otimes_{\mathbb{Z}} \mathbb{Q}$ est une algèbre de quaternions, et que E est supersingulière. Si $N \not\equiv -1 \pmod 4$, alors N se décompose dans $\mathbb{Z}[i]$, et il est facile de construire un point d'ordre p dans E , ce qui prouve que E est non supersingulière (cf [18] , 13,4, theorem 12). On étudie de façon analogue le cas $j = 0$. ∎

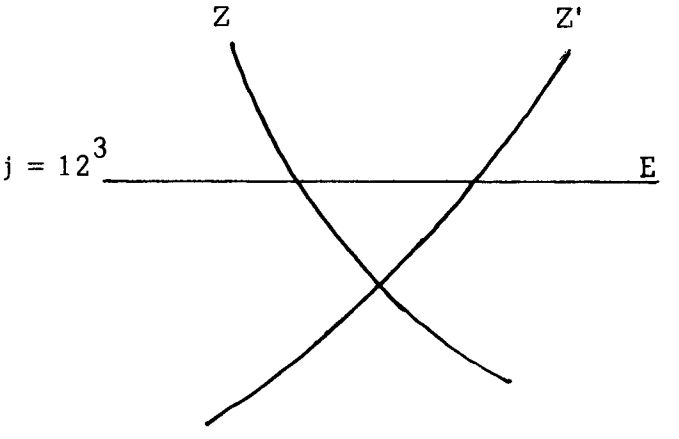
5.1.5. Considérons la courbe $\tilde{X}$ sur $\mathbb{F}_N$; si $N \equiv -1 \pmod 4$ (resp. $N \equiv -1 \pmod 6$) , on éclate le point supersingulier d'invariant $j = 12^3$ (resp $j = 0$) en une droite notée E (resp. en deux droites notées F et G , F coupant Z et G coupant Z') . (cf [1] , II,De-Ra,6,16).
Par exemple :

(i) $N = 11$ $(n=5)$: alors $N \equiv -1 \pmod 4$ et $N \equiv -1 \pmod 6$, donc les courbes d'invariant $j = 0$ et 12^3 sont supersingulières en réduction modulo N . Ce sont les seules, car $g+1 = 2$.



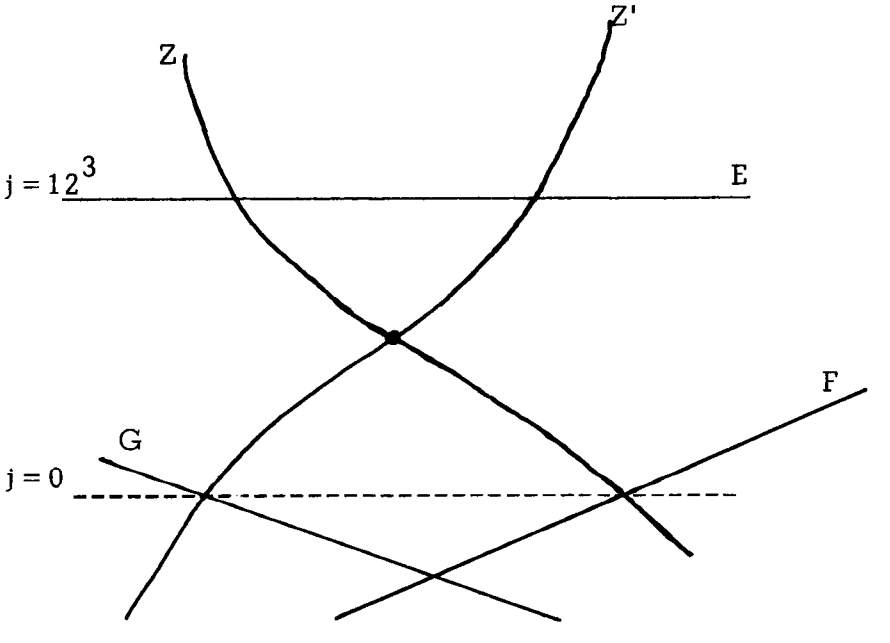
Par éclatement, on obtient un pentagone.

(ii) $N = 19$ $(n=3)$: alors $N \equiv -1 \pmod 4$ mais $N \not\equiv -1 \pmod 6$, donc la courbe d'invariant $j = 12^3$ est supersingulière, mais pas la courbe d'invariant $j = 0$. Comme $g + 1 = 2$, il y a un point supersingulier supplémentaire.



Par éclatement, on obtient un triangle.

(iii) $N = 23 \equiv -1$ (mod 4 et mod 6) ; $n = 11$. Comme pour $N = 11$, les invariants $j = 0$ et 12^3 donnent des points supersinguliers. Et il y en a un autre, car ici $g + 1 = 3$.



Par éclatement, on obtient un pentagone "croisé".

5.1.6. Nous avons vu en (I,4.2.3) que le genre g de X est égal à $[\frac{N+1}{12}]$ si $12 \nmid N-1$ et à $\frac{N-1}{12} - 1$ si $12 \mid N-1$. Nous allons calculer n , puis g en fonction de n , dans chacun des 4 cas qui interviennent ici, selon que $N+1$ est divisible ou non par 4 ou 6 .

LEMME . Soit N un nombre premier ≥ 5 .

(i) Si $N \not\equiv -1$ (mod 4) et $N \not\equiv -1$ (mod 6), alors $n = \frac{N-1}{12}$ et $g = n-1$;

(ii) Si $N \equiv -1 \pmod 4$ et $N \not\equiv -1 \pmod 6$, alors $n = \frac{N-1}{6}$ et $2g = n-1$;

(iii) Si $N \not\equiv -1 \pmod 4$ et $N \equiv -1 \pmod 6$, alors $n = \frac{N-1}{4}$ et $3g = n-1$;

(iv) Si $N \equiv -1 \pmod{12}$, alors $n = \frac{N-1}{2}$ et $6g = n+1$.

■ Puisque N est impair, on a $N \equiv -1 \pmod 4$ ou $N \equiv +1 \pmod 4$; donc $N-1$ est divisible par 4 si et seulement si $N \not\equiv -1 \pmod 4$. De même, puisque N n'est pas divisible par 3, on a $N \equiv -1 \pmod 3$ ou $N \equiv +1 \pmod 3$, donc $N-1$ est divisible par 3 (i.e. par 6) si et seulement si $N \not\equiv -1 \pmod 3$ (i.e. $\pmod 6$).

Ainsi, en (i), $N-1$ est divisible par 12 ; en (ii), $N-1$ est divisible par 6 mais pas par 12, n est impair, et $g = [\frac{n}{2}+\frac{1}{6}] = \frac{n-1}{2}$; en (iii), $N-1$ est divisible par 4 mais pas par 12, et $g = [\frac{N+1}{6} \times \frac{1}{2}] = \frac{N-5}{12} = \frac{n-1}{3}$; en (iv), $N-1$ n'est divisible ni par 4 ni par 6, et $g = \frac{N+1}{12} = \frac{n+1}{6}$. ■

5.1.7. Supposons $N \geq 5$. Nous savons que l'ensemble $\mathcal{C}$ des composantes de $\widetilde{X}$, après éclatement, est le suivant : (cf (5.1.4) et (5.1.6))

$\mathcal{C} = \{Z, Z'\}$ si $N \not\equiv -1 \pmod 4$ et $N \not\equiv -1 \pmod 6$ i.e. si $n = \frac{N-1}{12}$

$\mathcal{C} = \{Z, Z', E\}$ si $N \equiv -1 \pmod 4$ et $N \not\equiv -1 \pmod 6$ i.e. si $n = \frac{N-1}{6}$

$\mathcal{C} = \{Z, Z', F, G\}$ si $N \not\equiv -1 \pmod 4$ et $N \equiv -1 \pmod 6$ i.e. si $n = \frac{N-1}{4}$

$\mathcal{C} = \{Z, Z', E, F, G\}$ si $N \equiv -1 \pmod{12}$ i.e. si $n = \frac{N-1}{2}$.

Notons $\mathcal{D}$ le groupe abélien libre engendré par les composantes de $\widetilde{X}$; $\mathcal{D}^*$ le groupe dual "formel", i.e. le groupe abélien libre engendré par les symboles D^* pour D parcourant $\mathcal{C}$; α l'homomorphisme de $\mathcal{D}$ dans $\mathcal{D}^*$ défini par : $\alpha(\delta) = \sum_{D \in \mathcal{C}} (\delta . D) D^*$; β l'homomorphisme "degré" de $\mathcal{D}^*$ dans $\mathbb{Z}$ défini par : $\beta(\sum_{D \in \mathcal{C}} \alpha_D D^*) = \sum_{D \in \mathcal{C}} \alpha_D$; et $\mathcal{D}^*_o$ le noyau de β .

$$\mathcal{D} \xrightarrow{\alpha} \mathcal{D}^* \xrightarrow{\beta} \mathbb{Z} .$$

Nous allons voir que l'homomorphisme composé $\beta\circ\alpha$ est nul, c'est-à-dire que $\alpha(\mathcal{D})$ est contenu dans $\mathcal{D}^*_o$. Si D est une composante de $\widetilde{X}$, le produit d'intersection $(D.\widetilde{X})$ est nul. Donc, par linéarité, le produit d'intersection $(\delta.\widetilde{X})$ est nul pour tout $\delta \in \mathcal{D}$. Or $\beta\circ\alpha(\delta) = \sum_{D\in\mathcal{C}} (\delta.D) = (\delta.\widetilde{X})$; ainsi, $\beta\circ\alpha$ est nul et $\alpha(\mathcal{D})$ est un sous-groupe de $\mathcal{D}^*_o$.

PROPOSITION . <u>Le groupe $\mathcal{D}^*_o/\alpha(\mathcal{D})$ est cyclique d'ordre</u> n , <u>engendré par</u> $Z'^* - Z^*$.

■ (i) Calculons l'indice de $\alpha(\mathcal{D})$ dans $\mathcal{D}^*_o$, c'est-à-dire la valeur absolue du déterminant de la matrice carrée dont les coefficients sont les produits d'intersection $(D.D')$ pour D , D' parcourant tous les éléments, sauf un, de $\mathcal{C}$.

Calculons d'abord les produits d'intersection (D,D') pour $D \neq D'$: on voit immédiatement que : $(Z,E) = (Z,F) = (Z',E) = (Z',G) = (F,G) = 1$, que $(Z,G) = (Z',F) = (E,F) = (E,G) = 0$, et le lemme (5.1.3) donne $(Z,Z') = g+1$.

Calculons maintenant le produit d'intersection $(D.D)$, en remarquant qu'il est égal à l'opposé de $(D.(\widetilde{X}-D))$ puisque $(D.\widetilde{X}) = 0$. Si $E \in \mathcal{C}$, on a donc $(E.E) = -(E.(\widetilde{X}-E)) = -(E.Z) - (E.Z') = -2$; en effet, même si F et $G \in \mathcal{C}$, leur produit d'intersection avec E est nul. De même, $(F.F) = -(F.Z) - (F.G) = -2$ et $(G.G) = -(G.Z') - (G.F) = -2$. D'autre part, $(Z.Z) = -(Z.(\widetilde{X}-Z)) = -(Z.Z') = -(g+1)$, car le produit d'intersection ne change pas par éclatement. Et de même $(Z'.Z') = -(g+1)$.

Calculons maintenant l'indice de $\alpha(\mathcal{D})$ dans $\mathcal{D}^*_o$ c'est-à-dire la valeur absolue du déterminant de la matrice $((c,c'))_{c,c'\in\mathcal{C}-\{Z\}}$, et utilisons le lemme (5.1.6) :

Si $n = \frac{N-1}{12}$, $(\mathcal{D}^*_o:\alpha(\mathcal{D})) = |-(g/1)| = g+1 = n$

Si $n = \frac{N-1}{6}$, $(\mathcal{D}^*_o:\alpha(\mathcal{D})) = \left|\text{dét}\begin{pmatrix} -(g+1) & 1 \\ 1 & -2 \end{pmatrix}\right| = 2g+1 = n$

$$\text{Si } n = \frac{N-1}{4}\ ,\quad (\mathcal{B}_o^* : \alpha(\mathcal{B})) = \left|\det\begin{pmatrix} -(g+1) & 0 & 1 \\ 0 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix}\right| = 3g+1 = n$$

$$\text{Si } n = \frac{N-1}{2}\ ,\quad (\mathcal{B}_o^* : \alpha(\mathcal{B})) = \left|\det\begin{pmatrix} -(g+1) & 1 & 0 & 1 \\ 1 & -2 & 0 & 0 \\ 0 & 0 & -2 & 1 \\ 1 & 0 & 1 & -2 \end{pmatrix}\right| = 6g-1 = n\ .$$

Nous avons donc montré que $\mathcal{B}_o^*/\alpha(\mathcal{B})$ est d'ordre n .

(ii) Montrons maintenant que $\mathcal{B}_o^*/\alpha(\mathcal{B})$ est cyclique. Pour tout D dans $\mathcal{C}$, posons $\overline{D} = D^* - Z^*$. Alors $\mathcal{B}_o^*$ est le groupe abélien libre engendré par les symboles $\overline{D}$, pour D parcourant l'ensemble $\mathcal{C} - \{Z\}$, noté $\overline{\mathcal{C}}$. Et $\mathcal{B}_o^*/\alpha(\mathcal{B})$ est le quotient de ce groupe abélien libre par les relations : $\alpha(D) = 0$ pour tout $D \in \overline{\mathcal{C}}$; or $\alpha(D) = \sum_{D' \in \overline{\mathcal{C}}} (D.D').\overline{D'}$ par définition de α ; donc si $N \equiv -1 \pmod 4$, on a $\alpha(E) = \overline{Z'} - 2\overline{E}$, et si $N \equiv -1 \pmod 6$, on a $\alpha(F) = -2\overline{F} + \overline{G}$ et $\alpha(G) = \overline{Z'} + \overline{F} - 2\overline{G}$. Ainsi, si E (resp F , G) est dans $\mathcal{C}$, alors dans $\mathcal{B}_o^*/\alpha(\mathcal{B})$ on a : $\overline{E} = \frac{1}{2}\overline{Z'}$ (resp $\overline{F} = \frac{1}{3}\overline{Z'}$, $\overline{G} = \frac{2}{3}\overline{Z'}$) . Remarquons que (d'après (5.1.6)), $N \equiv -1 \pmod 4$ (resp.(mod 6)) si et seulement si n est impair (resp. n'est pas un multiple de 3), et qu'alors 2 (resp. 3) est bien inversible dans $\mathbb{Z}/n\mathbb{Z}$. En résumé, $\mathcal{B}_o^*/\alpha(\mathcal{B})$ est cyclique, de générateur $\overline{Z'}$, et la proposition est démontrée. ∎

5.1.8. Nous allons voir comment ce qui précède, joint à un résultat de M. Raynaud, permet de démontrer le théorème de Deligne admis en (3.1.2), que nous rappelons ci-dessous ; rappelons que $J_{/N}$ (resp. $J^c_{/N}$) désigne la fibre en N du schéma de Néron $J_{\mathbb{Z}}$ de J sur $\mathbb{Z}$ (resp. de la composante neutre $J^c_{\mathbb{Z}}$ de ce schéma) , et que $\overline{C}$ désigne la spécialisation de C en N (où C désigne le sous-groupe rationnel de J défini en (2.1)).

THEOREME. Le groupe $\overline{C}$ est cyclique d'ordre n , et l'on a : $J_{/N} \simeq \overline{C} \times J^c_{/N}$.

∎ D'après M. Raynaud (cf [29] ,6.1.3), le groupe quotient de

$J_{/N}$ par $J^c_{/N}$ est isomorphe au groupe $\mathcal{B}^*_o/\alpha(\mathcal{B})$ que nous venons d'étudier, l'isomorphisme étant induit par l'application suivante : à tout diviseur Δ de degré nul sur X, on fait correspondre l'élément $\sum_{D\in C} (\Delta\cdot D)D^* = \sum_{D\in\overline{C}} (\Delta\cdot D)\overline{D}$ de $\mathcal{B}^*_o$. L'image par cet isomorphisme de $(0)-(\infty)$ est donc la classe de $Z'^*-Z^* = \overline{Z}$ dans $\mathcal{B}^*_o/\alpha(\mathcal{B})$. Or $(0)-(\infty)$ (resp. $\overline{Z}$) est un générateur du groupe cyclique C (resp. $\mathcal{B}^*_o/\alpha(\mathcal{B})$), d'ordre n.

Ainsi, le quotient de $J_{/N}$ par $J^c_{/N}$ est la spécialisation $\overline{C}$ de C en N, et il est cyclique d'ordre n. ∎

5.2. $X(\mathcal{Q})$ EST REDUIT AUX POINTES ?

Nous avons indiqué dans le paragraphe 4 comment Mazur a montré que $X(\mathcal{Q})$ est fini (cf [21]) ; Ogg a conjecturé que $X(\mathcal{Q})$ est réduit à ses deux pointes si N est suffisamment grand. Nous discutons ci-dessous cette conjecture et la démontrons sous l'hypothèse : $J_-(\mathcal{Q})$ est fini (cf 5.2.6).

5.2.1. *LEMME*. Soit P un point de $X(\mathcal{Q})$. Alors il existe un nombre m dans $\{0,1,1/2,1/3,2/3\}$ tel que les images de $(P)-(\infty)$ et $m((0)-(\infty))$ dans le quotient $J_{/N}/J^c_{/N}$ soient égales. De plus, on ne peut avoir $m = 1/2$ (resp. $m = 1/3$ ou $m = 2/3$) que si $N \equiv -1 \pmod 4$) (resp. $N \equiv -1 \pmod 6$).

∎ On peut montrer (cf [1], II, De-Ra) que la section du schéma $J_{\mathbb{Z}}$ correspondant à un point quelconque P de $X(\mathcal{Q})$ coupe une et une seule composante (notée D_P) de la fibre en N, et que cette intersection est simple. Ainsi, dans l'isomorphisme entre $J_{/N}/J^c_{/N}$ et $\mathcal{B}^*_o/\alpha(\mathcal{B})$ explicité en (5.1.8), l'image de $(P)-(\infty)$ est égale à $D^*_P - Z^* = \overline{D}_P$. D'après (5.1.7), on a : $\overline{Z} = 0$, $\overline{E} = \frac{1}{2}\overline{Z}'$, $\overline{F} = \frac{1}{3}\overline{Z}'$, $\overline{G} = \frac{2}{3}\overline{Z}'$, et de plus E (resp. F et G) n'existe que si $N \equiv -1 \pmod 4$ (resp $N \equiv -1 \pmod 6$). ∎

5.2.2. *PROPOSITION*. Si $J_-(\mathbb{Q})$ est fini, alors

(i) $J_-(\mathbb{Q}) = C$;

et

(ii) si P est un point de $X(\mathbb{Q})$, il existe un nombre $\ell = \ell(P)$ dans $\{-1, 1, 0, -\frac{1}{3}, \frac{1}{3}\}$ tel que $(P) - (WP)$ et $\ell((0)-(\infty))$ soient égaux dans C. De plus, on ne peut avoir $\ell = 0$ (resp $\ell = \pm\frac{1}{3}$) que si $N \equiv -1 \pmod 4$ (resp. $N \equiv -1 \pmod 6$).

■ (i) On a toujours $C \subset J_-(\mathbb{Q})$ (cf 2.3.3) ; d'autre part, si $J_-(\mathbb{Q})$ est fini, il est dans le groupe de torsion de $J(\mathbb{Q})$, qui est égal à C d'après (3.2.4).

(ii) Considérons le diviseur

$$((P) - (WP)) + ((0) - (\infty)) = ((P) - (\infty)) - W((P) - (\infty)) .$$

D'après le lemme (5.2.1), $(P) - (\infty)$ a même image dans $\overline{C}$ que $m((0)-(\infty))$ pour un m dans $\{0, 1, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}\}$. Comme W échange les pointes 0 et ∞, l'image de $(P) - (WP) + (0) - (\infty)$ est la même que celle de $2m((0)-(\infty))$. Posons $\ell = 2m-1$: ainsi $(P) - (WP)$ et $\ell((0)-(\infty))$ ont même image dans $\overline{C} \simeq C$ et ℓ est dans l'ensemble $\{-1, 1, 0, -\frac{1}{3}, \frac{1}{3}\}$; les restrictions indiquées dans le proposition sont celles du lemme (5.2.1).

D'autre part, $(P) - (WP)$ est dans C : en effet, il est dans $J_-(\mathbb{Q})$ (cf 2.3.3), et d'après (i), $J_-(\mathbb{Q}) = C$. Donc les diviseurs $(P) - (WP)$ et $\ell((0) - (\infty))$ sont égaux. ■

5.2.3. Notons Φ l'application de X dans J_- qui associe au point P la classe du diviseur $(P) - (WP)$ dans J.

PROPOSITION (cf Ogg [32]) : Si $N \geq 23$ et $N \neq 37$, l'application Φ est injective en dehors des points fixes de W.

■ Remarquons d'abord que tous les points fixes de W ont une image nulle. Soient maintenant P et Q deux points distincts de X, tels

que $\phi(P) = \phi(Q)$, et supposons $P \neq WP$. Il existe alors une fonction f dans $\mathbb{C}(X)$ de diviseur $(f) = ((P) + (WQ)) - ((Q)+(WP))$; et comme $P \neq Q$, et $P \neq WP$, la fonction f est vraiment de degré 2 . Ainsi, d'après (1.3), X est une courbe hyperelliptique. Soit v l'involution hyperelliptique ; elle transforme un zéro de f en l'autre, autrement dit $vWQ = P$. Si $v = W$, alors $P = Q$, ce qui est contraire à l'hypothèse ; donc $v \neq W$, et $N = 37$ d'après (1.3.4). ∎

5.2.4. *PROPOSITION.* Si l'involution d'Atkin-Lehner sur X a un point fixe rationnel sur $\mathbb{Q}$, alors $N = 11,19,43,67$ ou 163.

∎ Nous avons vu en (1.2.3) que les points fixes de W sur X correspondent aux couples (E,λ) tels que $\lambda = \sqrt{-N}$, c'est-à-dire aux courbes elliptiques à multiplication complexe par $\sqrt{-N}$. De telles courbes existent toujours sur $\overline{\mathbb{Q}}$ (leur nombre w a été calculé en (1.2.3)), nous allons voir dans quels cas il peut en exister sur $\mathbb{Q}$.

Soient $\mathcal{O}$ un ordre de $\mathbb{Q}(\sqrt{-N})$ contenant $\sqrt{-N}$, E une courbe elliptique d'anneau des endomorphismes $\mathcal{O}$; alors E est isomorphe à $\mathbb{C}/\mathfrak{a}$, pour un $\mathcal{O}$-idéal propre $\mathfrak{a}$ (cf II,5.3.3). Notons j l'invariant de E , et $h_{\mathcal{O}}$ le nombre de classes de $\mathcal{O}$-idéaux propres. Nous savons, par la théorie de la multiplication complexe (cf II,5.3.4), que l'extension $\mathbb{Q}(\sqrt{-N})(j)/\mathbb{Q}(\sqrt{-N})$ est de degré $h_{\mathcal{O}}$. Si E est défini sur $\mathbb{Q}$, alors $j \in \mathbb{Q}$ et $h_{\mathcal{O}} = 1$. Comme le nombre de classes d'un ordre est au moins égal au nombre de classes de l'ordre maximal, le corps $\mathbb{Q}(\sqrt{-N})$ doit avoir un nombre de classes égal à 1 . Autrement dit, $\mathbb{Q}(\sqrt{-N})$ est l'un des 9 corps de Gauss, qui correspondent à $N = 1,2,3,7,11,19,43,67,163$ (cf [5a] ,13). Comme nous avons supposé $N \geq 11$ (c'est-à-dire X de genre ≥ 1) , la proposition est démontrée. ∎

Remarque : un raisonnement analogue prouve, plus généralement, le résultat suivant :

si l'involution d'Atkin-Lehner sur X a un point fixe rationnel sur un corps de nombres K , alors le nombre de classes de

$\mathbb{Q}(\sqrt{-N})$ divise le degré de l'extension $K\mathbb{Q}(\sqrt{-N})/\mathbb{Q}(\sqrt{-N})$.

C'est ce résultat que nous avons utilisé en (4.3.2) pour un corps quadratique imaginaire K .

5.2.5. Remarquons que $\ell(0) = 1$ et $\ell(\infty) = -1$. Et que, d'après (5.2.2), s'il existe $P \in X(\mathbb{Q})$ tel que $\ell(P) = 0$ (resp. $\ell(P) = \pm\frac{1}{3}$) , alors $N \equiv -1 \pmod 4$ (resp. $N \equiv -1 \pmod 6$) .

Si l'on suppose de plus que $J_-(\mathbb{Q})$ est fini, on obtient des conditions supplémentaires liant N et les valeurs prises par $\ell(P)$:

PROPOSITION (cf [22]). Si $J_-(\mathbb{Q})$ est fini, et s'il existe un point P de $X(\mathbb{Q})$, distinct des pointes, tel que

(i) $\ell(P) = 0$, alors $N = 11, 19, 43, 67$ ou 163 ;

(ii) $\ell(P) = \pm\frac{1}{3}$, alors $N = 11$ ou 17 ;

(iii) $\ell(P) = \pm 1$, alors $N = 37$.

■ D'après ce qui précède (cf 5.2.2) les diviseurs $(P) - (WP)$ et $\ell(P)((0) - (\infty))$ sont égaux dans C .

(i) Si $\ell(P) = 0$,alors $(P) - (WP)$ est le diviseur d'une fonction. Le genre de X étant ici non nul, il n'y a pas de fonction sur X de degré 1 . Cela implique que $P = WP$, et la proposition (5.2.4) permet de conclure.

(ii) Si $\ell(P) = \frac{1}{3}$, alors $3((P)-(WP)) - ((0)-(\infty))$ est le diviseur d'une fonction f de $\mathbb{Q}(X)$ de degré 4 . En fait, cette fonction induit une fonction $\tilde{f}$ de $\mathbb{F}_4(\tilde{X})$ de degré 4 et donc définit un revêtement de degré 4 : $\tilde{X}(\mathbb{F}_4) \to \mathbb{P}^1(\mathbb{F}_4)$; ainsi, $\tilde{X}(\mathbb{F}_4)$ a au plus 20 points. Mais nous savons que $\tilde{X}(\mathbb{F}_4)$ a au moins $(\frac{N+1}{12} + 2)$ points (cf 1.1.3). D'où $N \leq 195$. D'autre part, on doit avoir $N \equiv -1 \pmod 6$ (cf 5.2.2) . Considérons la fonction $f \circ W$, son diviseur vaut $(f \circ W) = -(f)$, donc f et $\frac{1}{f \circ W}$ sont proportionnels. La constante $C = f \times (f \circ W)$ est non nulle (et elle est rationnelle car $f \in \mathbb{Q}(X)$ et W est définie sur $\mathbb{Q}$). La fonction

$f^2 - C = f[f-f\circ W]$ est de degré 8 , et tous les points fixes de W dans X l'annulent.

Donc le nombre ω de points fixes de W doit être inférieur ou égal à 8 . Nous avons calculé ω en (1.2.3) ; nous devons donc avoir, en notant h le nombre de classes de $\mathbb{Q}(\sqrt{-N})$: $h = h(-4N) \leq 8$ si $N \equiv 1 \pmod 4$, $h = h(-N) \leq 4$ si $N \equiv 7 \pmod 8$, et $h = h(-N) \leq 2$ si $N \equiv 3 \pmod 8$.

Les nombres premiers $N \geq 11$ vérifiant toutes ces conditions sont les nombres : 11,17,23,29,41,53,113,137, comme le montre le tableau ci-dessous. On peut montrer, par d'autres méthodes, que les valeurs 23, 29,41,53,113 et 137 ne conviennent pas, d'où le résultat (nous allons étudier en (5.3) les cas $N = 23,53,41$; dans un article à paraître au Journal de Théorie des Nombres, Parry étudie les cas $N = 53,113,137$) .

Ce tableau indique, pour tous les nombres premiers N entre 11 et 193 , la classe de N mod.6 , puis mod.8 , et le nombre de classes h de $\mathbb{Q}(\sqrt{-N})$. Les lettres a,b,c,d lues dans la dernière colonne, ont la signification suivante :

a - $N \not\equiv -1 \pmod 6$

b - $N \equiv 1 \pmod 4$ et $h > 8$

c - $N \equiv 7 \pmod 8$ et $h > 4$

d - $N \equiv 3 \pmod 8$ et $h > 2$.

N	N mod.6	N mod.8	h	
11	-1	3	1	
17	-1	1	4	
19	1	3	1	a
23	-1	7	3	
29	-1	5	6	
31	1	7	3	a
37	1	5	2	a
41	-1	1	8	
43	1	3	1	a
47	-1	7	5	c
53	-1	5	6	
59	-1	3	3	d

N	N mod.6	N mod.8	h	
61	1	5	6	a
67	1	3	1	a
71	-1	7	7	c
73	1	1	4	a
79	1	7	5	a,c
83	-1	3	3	d
89	-1	1	12	b
97	1	1	4	a
101	-1	5	14	b
103	1	7	5	a,c
107	-1	3	3	d
109	1	5	6	a
113	-1	1	8	
127	1	7	5	a,c
131	-1	3	5	d
137	-1	1	8	
139	1	3	3	a,d
149	-1	5	14	b
151	1	7	7	a,c
157	1	5	6	a
163	1	3	1	a
167	-1	7	11	c
173	-1	5	14	b
179	-1	3	5	d
181	1	5	10	a,b
191	-1	7	13	c
193	1	1	4	a

(iii) Lorsque $N = 11$ (resp. $N = 17$, resp. $N = 19$), nous avons déjà obtenu 5 (resp. 4, resp. 3) valeurs distinctes pour $\ell(P)$; ce nombre étant égal à n , nous avons obtenu toutes les valeurs possibles pour $\ell(P)$, et nous pouvons supposer maintenant : $g \geq 2$; (en fait, lorsque $N = 17$, on a $\pm\frac{1}{3} \equiv \mp 1 \pmod{n}$) .

Si $\ell(P) = 1$, alors $(P) + (\infty) - (WP) - (0)$ est le diviseur d'une fonction f de $\mathbb{Q}(X)$ de degré 2 . (nous avons supposé $P \neq 0,\infty$). Donc X est une courbe hyperelliptique, et l'involution hyperelliptique v est telle que $v(P) = \infty \neq W(P)$ (cf 1.3.1) ; d'après (1.3.4), ce n'est possible que pour $N = 37$. ∎

Remarque (cf [22] ,3.3) : Réciproquement, si $N = 11,19,43,67$ ou 163 (resp. $N = 11$ ou 17 , resp. $N = 37$), il existe un point P de $X(\mathbb{Q})$

tel que $\ell(P) = 0$ (resp. $\ell(P) = \frac{1}{3}$, resp. $\ell(P) = 1$) .

5.2.6. *THEOREME*. Si $J_-(\mathbb{Q})$ est fini, et $N \neq 11,17,19,37,43,67,163$, alors les seuls points rationnels de X sont les pointes 0 et ∞ .

▪ Il suffit de regrouper les résultats obtenus en (5.2.2) et (5.2.5). ▪

Remarques :

(i) Les calculs faits par Brumer et Kramer pour $N < 250$ montrent que, si $N \neq 151$, 227 , on a $J^- = \mathcal{J}$, ou bien $J^- = \mathcal{J} \times E$ où E est une courbe elliptique de conducteur N avec un nombre fini de points rationnels. Comme on a montré que $\mathcal{J}(\mathbb{Q})$ est fini (en 4.2.1), et que J_- et J^- sont isogènes (en 2.0), le théorème s'applique pour toutes ces valeurs de N .

(ii) On trouve dans [22] une table donnant pour les nombres premiers $N < 250$: la valeur de n , la dimension des facteurs qui composent J_+ (resp. J_- , $\mathcal{J}$) , le nombre de points de $X(\mathbb{Q})$ différents des pointes, et les valeurs prises par $\ell(P)$ (cf 5.2.5).

5.3. EXEMPLES : $N = 23$, 41 , 53 .

5.3.1. Pour conclure, vérifions le résultat suivant (admis en 5.2.5) :

PROPOSITION . Lorsque $N = 23$, 53 ou 41 , les seuls points rationnels de la courbe modulaire $X_0(N)$ sont ses deux pointes.

Lorsque $N = 23$ ou 53 , on utilise la théorie de la multiplication complexe (cf II,5.3) :

▪ D'après (5.2.5 (ii)) , il suffit de montrer que le nombre $\ell(P)$ ne peut pas prendre la valeur $1/3$, c'est-à-dire qu'il ne peut pas exister

une fonction f dans $\mathbb{Q}(X)$, de degré 4 , telle que $f.f\circ W$ soit une constante rationnelle non nulle (notée C) .

Supposons qu'une telle fonction f existe, alors la fonction f^2-C est de degré 8 , et les points fixes par W l'annulent car $f^2-C = f(f-f\circ W)$. Nous avons étudié en (1.2.3) les points de $X_0(N)$ fixes par W : ils sont dans $Y_0(N)$, et sont représentés par les couples (E,λ) tels que : End E contient $\sqrt{-N}$, et $\lambda = \sqrt{-N}$. En particulier, si End E est égal à l'ordre maximal $\mathcal{O}$ du corps $K = \mathbb{Q}(\sqrt{-N})$, le couple $(E,\sqrt{-N})$ définit un point de $X_0(N)$ fixe par W .

Or (cf II,5.3.3) l'ensemble des idéaux de K est en bijection avec l'ensemble des classes de courbes elliptiques E telles que End $E \simeq \mathcal{O}$, la bijection étant définie par : $\mathfrak{a} \to \mathbb{C}/\mathfrak{a}$. Notons $P(\mathfrak{a})$ le point de $X_0(N)$ représenté par le couple $(\mathbb{C}/\mathfrak{a},\sqrt{-N})$; c'est un point fixe par W , donc : $f(P(\mathfrak{a})) = \pm\sqrt{C}$.

D'autre part (cf II,5.3.4) , l'extension $K(j(\mathcal{O}))/K$ est galoisienne, son degré est égal au nombre de classes de K (noté h) , et les conjugués de $j(\mathcal{O})$ sur K sont les nombres $j(\mathfrak{a})$, lorsque $\mathfrak{a}$ parcourt l'ensemble des classes d'idéaux de K . On a donc une bijection entre l'ensemble des points de $X_0(N)$ de la forme $P(\mathfrak{a})$, et les conjugués de $j(\mathcal{O})$ sur K , bijection définie par : $P(\mathfrak{a}) \to j(\mathfrak{a})$; et la fonction f , définie sur $X_0(N)$ et rationnelle sur $\mathbb{Q}$, induit une fonction g , définie sur l'ensemble des conjugués de $j(\mathcal{O})$ sur $\mathbb{Q}$, et rationnelle sur $\mathbb{Q}$, par : $g(j(\mathfrak{a})) = f(P(\mathfrak{a}))$.

Soit σ un $\mathbb{Q}$-automorphisme de $\overline{\mathbb{Q}}$ tel que $(\sqrt{c})^\sigma = -\sqrt{c}$; soient $\mathfrak{a}$, $\mathfrak{b}$, deux idéaux de K tels que $j(\mathfrak{a})^\sigma = j(\mathfrak{b})$; comme g est rationnelle sur $\mathbb{Q}$, on a : $g(j(\mathfrak{b})) = (g(j(\mathfrak{a})))^\sigma$; et comme $g(j(\mathfrak{a})) = f(P(\mathfrak{a})) = \pm\sqrt{c}$, cela donne : $g(j(\mathfrak{b})) = -g(j(\mathfrak{a}))$. Ce raisonnement permet de diviser l'ensemble des conjugués de $j(\mathcal{O})$ sur K en deux sous-ensembles de même cardinal selon que $g(j(\mathfrak{a})) = +\sqrt{c}$ ou $-\sqrt{c}$.

Lorsque $N = 23$, le nombre de classes h est égal à 3 , donc le nombre de conjugués de $j(\mathcal{O})$ sur K est impair, et ce qui précède prouve qu'il ne peut pas exister de fonction du type de f ; donc $X_0(23)(\mathbb{Q})$

est réduit aux deux pointes.

Lorsque $N = 53$, le nombre de classes h est égal à 6 , et les points de $X_o(53)$ fixes par W sont les six points $P(\mathfrak{C}_i)$ $(1 \leq i \leq 6)$ correspondant aux six classes d'idéaux de K (car $N \equiv 1 \pmod 4$, donc $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-N}$ est le seul ordre de K contenant $\sqrt{-N}$; cf(1.2.3)) . Parmi ces six points, trois annulent $f - \sqrt{c}$, et trois annulent $f + \sqrt{c}$; or chacune de ces fonctions est de degré 4 , donc il existe deux points Q_1 et Q_2 de $X_o(N)$ qui ne sont pas fixes par W et tels que $f(Q_1) = +\sqrt{c}$ et $f(Q_2) = -\sqrt{c}$. Ainsi, Q_1 est racine de $f^2 - C$; comme $C = f.f\circ W$, cela prouve que WQ_1 est lui aussi racine de $f^2 - C$, donc que $WQ_1 = Q_2$. Mais alors, d'une part $f(Q_1).f(WQ_1) = f.f\circ W(Q_1) = C$, et d'autre part $f(Q_1).f(WQ_1) = f(Q_1).f(Q_2) = (\sqrt{c})(-\sqrt{c}) = -C$. Dans ce cas aussi, il ne peut pas exister de telle fonction f , et $X_o(53)(\mathbb{Q})$ est réduit à ses deux pointes. ∎

5.3.2. Le cas $N = 41$.

Nous utilisons ici une méthode différente des deux cas précédents. En fait, nous allons étudier la réduction $\tilde{X}$ modulo 7 de $X_o(41)$, et montrer que $\tilde{X}(\mathbb{F}_7)$ est réduite aux pointes.

Nous utilisons pour cela le lemme suivant :

Soient p un nombre premier différent de 2 et de N , f un entier positif, $q = p^f$; soient E une courbe elliptique sur $\mathbb{F}_q$, $\pi = \pi_q$ son endomorphisme de Frobenius, $\pi' = \pi'_q$ l'endomorphisme transposé, s l'entier égal à $\pi + \pi'$ (cf II,5.2.3) , et $-d = s^2 - 4q$ le discriminant du polynôme $(X-\pi)(X-\pi') = X^2 - sX + q$. Nous avons vu en (II,5.2.3) que d est positif ou nul.

LEMME . (i) La courbe E est supersingulière si et seulement si p divise d ;

(ii) La courbe E a un sous-groupe C cyclique d'ordre N rationnel sur $\mathbb{F}_q$ si et seulement si $(\frac{-d}{N}) = 1$.

■ (i) Toutes les assertions suivantes sont équivalentes : E est supersingulière ; π' est inséparable ; π'_* annule les différentielles (cf II,5.4.1) ; s_* annule les différentielles (car $s_* = \pi_* + \pi'_*$, et π est toujours inséparable) ; p divise s (car p est le seul nombre premier définissant une isogénie inséparable) ; p divise d (car $d = 4p^f - s^2$).

(ii) Supposons que E a un sous-groupe C cyclique d'ordre N et rationnel sur $\mathbb{F}_q$, c'est-à-dire invariant par π . Notons c un générateur de C , et a l'entier (déterminé modulo N , et non nul modulo N) tel que : $\pi c = ac$. Alors C est annulé par $\pi - a$, donc par $(\pi' - a)(\pi - a) = a^2 - sa + q$; autrement dit, le polynôme $(X^2 - sX + q)$ a un zéro dans $\mathbb{F}_N^*$, ce qui prouve que son discriminant $(-d)$ est un carré modulo N .

Réciproquement, si $(\frac{-d}{N}) = 1$, l'équation $(X^2 - sX + q)$ a des racines dans $\mathbb{F}_N$; considérons l'espace vectoriel E_N de dimension 2 sur $\mathbb{F}_N$ (rappelons que $p \neq N$), et considérons π comme un endomorphisme de E_N; ses valeurs propres sont rationnelles, donc le sous-groupe de E engendré par un de ses vecteurs propres est rationnel sur $\mathbb{F}_q$ et d'ordre N . ■

En appliquant la dernière assertion de ce lemme au cas : $N = 41$, $p = q = 7$, nous montrons ci-dessous que $X_o(41)(\mathbb{Q})$ est réduit aux deux pointes :

■ Montrons d'abord que la réduction (mod.7) de $Y_o(41)$ n'a pas de point rationnel sur $\mathbb{F}_7$, c'est-à-dire que $\widetilde{Y_o(41)}(\mathbb{F}_7)$ est vide ; les couples d'entiers positifs (d,s) tels que : $d = 4.7 - s^2$ sont au nombre de 6 . Le tableau ci-dessous donne les valeurs de : s , d , $(\frac{-d}{N})$.

s	d	$(\frac{-d}{N})$
0	28	-1
1	27	-1
2	24	-1
3	19	-1
4	12	-1
5	3	-1

Comme $\widetilde{(\frac{-d}{N})}$ est toujours égal à -1 , la partie (ii) du lemme prouve que $\widetilde{Y_o(41)}(\mathbb{F}_7)$ est vide.

Considérons maintenant l'application de X dans J définie par : $P \longmapsto (P) - (WP)$; nous avons étudié cette application en (5.2.3) : c'est une application de X dans J_- , qui est injective en dehors des points fixes de W lorsque $N = 41$; or il n'y a pas de point fixe par W sur $X_o(41)(\mathbb{Q})$ (cf 5.2.4), et on obtient ainsi une injection de $X_o(41)(\mathbb{Q})$ dans $J_o(41)_-(\mathbb{Q})$. Considérons le diagramme suivant :

$$\begin{array}{ccc} X_o(41)(\mathbb{Q}) & \hookrightarrow & J_o(41)_-(\mathbb{Q}) \\ \downarrow & & \downarrow \\ \widetilde{X_o(41)}(\mathbb{F}_7) & \longrightarrow & \widetilde{J_o(41)_-}(\mathbb{F}_7) \end{array}$$

il est commutatif d'après (II,6.4) ; de plus, $J^- = \mathcal{J}$ lorsque $N = 41$ (cf [22]), donc $J_-(\mathbb{Q})$ est de torsion, comme $\mathcal{J}(\mathbb{Q})$ (cf 4.2.1 et 2.0). Or le groupe de torsion de $J(\mathbb{Q})$ est égal à C (cf 3.2.4), et l'ordre de C est égal à $n = 10$; donc l'ordre de $J_-(\mathbb{Q})$ est premier à 7 , et la réduction : $J_-(\mathbb{Q}) \to \widetilde{J}_-(\mathbb{F}_7)$ est injective.

En résumé, l'application : $X(\mathbb{Q}) \hookrightarrow J_-(\mathbb{Q}) \hookrightarrow \widetilde{J}_-(\mathbb{F}_7)$ est injective, et égale à l'application : $X(\mathbb{Q}) \to \widetilde{X}(\mathbb{F}_7) \to \widetilde{\mathcal{J}}(\mathbb{F}_7)$; donc le cardinal de $X(\mathbb{Q})$ est au plus égal à celui de $\widetilde{X}(\mathbb{F}_7)$, et $X(\mathbb{Q})$ a exactement deux éléments. ∎